serie de matemática monografia no. 3

ESTRUCTURAS ALGEBRAICAS

Departamento de Asuntos Científicos
Unión Panamericana - Secretaría General
Organización de los Estados Americanos



ESTRUCTURAS ALGEBRAICAS

por

ENZO R. GENTILE

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Buenos Aires, Argentina

Departamento de Asuntos Científicos
Unión Panamericana
Secretaría General
Organización de los Estados Americanos
Washington, D.C. - 1967

Esta monografía ha sido preparada para su publicación en el Departamento de Asuntos Científicos de la Unión Panamericana

Editora: Eva V. Chesneau

NOTA DE INTRODUCCION

La colección de monografías científicas forma parte de los programas generales de información y publicaciones del Departamento de Asuntos Científicos y tiene como finalidad principal difundir y presentar de manera sencilla los nuevos temas y métodos que surgen del rápido desarrollo de las ciencias y de la tecnología.

En la actualidad la colección consta de cuatro series, en español y portugués, sobre física, química, biología y matemática, pero se contempla la posibilidad de incluir otros ramos de las ciencias.

Desde su comienzo se dedicó estas monografías a los profesores y estudiantes de ciencias de nivel secundario y universitario básico, no obstante se aspira a que encuentren también acogida entre los hombres de ciencias dedicados a la investigación especializada y el público en general que se interese en adquirir información o conocimientos sobre la materia.

En esta oportunidad, la Unión Panamericana agradece a la Agencia para el Desarrollo Internacional y a la Fundación Nacional de Ciencias de los Estados Unidos por la significativa ayuda económica recibida en apoyo de este programa, así como al Dr. Enzo R. Gentile, autor de la monografía, y al Prof. Gerardo Ramos del Instituto de Matemáticas Puras y Aplicadas, Universidad Nacional de Ingeniería, Lima, Perú, por la revisión técnica del manuscrito.

Jesse D. Perkinson
Director

PROLOGO

El profesor Enzo Gentile, bien conocido en los medios educativos latinoamericanos por sus interesantes libros de álgebra, ha escrito a petición de la Unión Panamericana esta obra de introducción a dicha materia.

Es inútil referirse a todas las cualidades de la monografía, que son muchas, pues pronto el lector las apreciará por sí mismo. Pero si debe advertirse que, aun siendo elemental, el tratamiento es profundo, como lo requiere el estado presente de estas disciplina. El autor no ha intentado cubrir abundante material, sino que se ha limitado a caracterizar lo esencial de las estructuras básicas del álgebra. Sin embargo, todos los conceptos están ligados por principios unificadores de modo que una estructura sigue naturalmente a la otra en un proceso de evolución y de creciente diversificación. Gran parte de las ideas básicas están referidas a estructuras simples y sus morfismos: los monoides y los semigrupos. Estas ideas son objeto de sucesivas adaptaciones a medida que el desenvolvimiento de las estructuras lo exige a consecuencia de la definición de nuevas relaciones, tales como las de equivalencia, que conducen a las estructuras cocientes.

Los numerosos ejemplos y ejercicios forman parte importante del texto. Estos han sido cuidadosamente seleccionados para ilustrar conjuntos de propiedades, enriquecer matices, destacar importantes analogías y penetrar en campos afines de mucho interés.

Finalmente, conviene prevenir al lector que se inicia en el estudio del álgebra que con esta monografía del profesor Gentile no sólo llegará a familiarizarse con conceptos de gran valor, sino que, además, los encontrará expresados en el lenguaje del álgebra de hoy, es decir, en términos de diagramas conmutativos, morfismos,

biyecciones y sucesiones exactas. Esta es, sin duda, una de sus características más ventajosas para vencer desde el comienzo la barrera que artificialmente pudiera crear el nuevo lenguaje.

Gerardo Ramos

Lima, Perú, junio de 1967

INDICE

INTRODUCCION

En este capítulo se establecerán los conceptos que pueden considerarse como prerequisitos para la lectura de esta monografía. La exposición es puramente enumerativa y se supone que el lector esté familiarizado con el material.

A. Lógica Proposicional

Se entiende por proposición una sentencia con un único valor de verdad: **V** = verdadero o **F** = falso.

El sentido de "verdad" en una teoría matemática es el siguiente: una proposición P es verdad (o verdadera) si es un axioma de la teoría o si es demostrable, por reglas válidas de razonamiento, a partir de los axiomas de la teoría. O sea, brevemente, el sentido de verdad es el de "demostrable".

Sean P y Q proposiciones. Se tienen las siguientes proposiciones asociadas:

$$\begin{aligned} P' &= \text{negación de } P \\ P \cdot Q &= P \text{ y } Q \\ P \text{ o } Q &= P \text{ o } Q \end{aligned}$$

Los valores de verdad de estas nuevas proposiciones están dados por las tablas de verdad, reunidas en una,

P	Q	- P	P·Q	P o Q
V	**V**	**F**	**V**	**V**
V	**F**	**F**	**F**	**V**
F	**V**	**V**	**F**	**V**
F	**F**	**V**	**F**	**F**

Leyes de De Morgan

$$\begin{aligned} (P \text{ o } Q)' &= P' \cdot Q' \\ (P \cdot Q)' &= P' \text{ o } Q' \end{aligned}$$

Por igualdad = debe entenderse que para cada asignación de valor de verdad a P y Q, $(P \text{ o } Q)'$ y $P' \cdot Q'$ poseen el mismo valor de verdad y, análogamente, $(P \cdot Q)'$ y P' o Q'. O sea, la igualdad radica en poseer las mismas tablas de verdad.

La proposición P' o Q posee la siguiente tabla de verdad

P	Q	P' o Q
V	**V**	**V**
V	**F**	**F**
F	**V**	**V**
F	**F**	**V**

En matemática se utiliza esta proposición para representar el condicional: si P entonces Q. Se la denota por

$$P \Rightarrow Q$$

y se lee: P implica Q. P se denomina el antecedente del condicional y Q el consecuente. El lector puede observar que el hecho que $P \Rightarrow Q$ sea **V** no da ninguna información sobre los valores de verdad del antecedente o del consecuente. Esta situación es satisfactoria en matemática y en toda ciencia deductiva. Por ejemplo, las proposiciones siguientes son verdaderas:

$$-1 = 1 \Rightarrow 1 = 1$$
$$-1 = 1 \Rightarrow 2 = 0$$

2 La forma en que se utiliza en matemática el condicional $P \Rightarrow Q$ es la siguiente. A partir de una proposición P (verdadera o falsa), y utilizando reglas válidas de razonamiento, deducimos una proposición Q. O sea, utilizando la terminología matemática deducimos Q de P. Es evidentemente que de acuerdo con lo que significa una deducción no puede un razonamiento matemático deducir una proposición falsa de una proposición verdadera. O sea que, independientemente del valor de verdad de P, la proposición $P \Rightarrow Q$ es verdadera. Ahora bien, si ocurre que P es **V** entonces, observando la tabla de verdad de $P \Rightarrow Q$, se tiene que Q es **V**. Esta regla de inferencia se denomina *modus ponens* y se expresa brevemente por

$$\text{Si } \left\{ \begin{array}{l} P \Rightarrow Q \text{ es } \mathbf{V} \text{ y} \\ P \text{ es } \mathbf{V} \end{array} \right\} \text{ entonces } Q \text{ es } \mathbf{V}.$$

Otras denominaciones para la proposición $P \Rightarrow Q$ son:

P, sólo si Q, P es condición suficiente para Q.
Q, si P, Q es condición necesaria para P.

Así, "una condición necesaria (pero no suficiente) para que un triángulo sea equilátero es que sea un triángulo isósceles" y "una condición suficiente (pero no necesaria) para que un triángulo sea isósceles es que sea un triángulo equilátero".

La proposición

$$(P \Rightarrow Q) \cdot (Q \Rightarrow P)$$

la denotamos por

$$P \Leftrightarrow Q$$

y se denomina: P es equivalente a Q o P si, y sólo si, Q o P es condición necesaria y suficiente para Q. $P \Leftrightarrow Q$ es **V** si P y Q poseen simultáneamente el mismo valor de verdad.

Por ejemplo, la siguiente es una proposición verdadera

$$(P \Rightarrow Q) \Leftrightarrow (Q' \Rightarrow P')$$

Por tanto, $P \Rightarrow Q$ y $Q' \Rightarrow P'$ son simultáneamente verdaderas o falsas. Este hecho lo utilizaremos a menudo para probar la validez de $P \Rightarrow Q$, probando la validez de $Q' \Rightarrow P'$. Este tipo de demostración lo llamaremos reducción al absurdo.

B. Conjuntos

Sea X un conjunto. Con $x \in X$ denotamos la proposición "x es un elemento de X" o "x pertenece a X" o también "X contiene a x". Con $x \notin X$ denotamos su negación.

Sean Z, Y conjuntos. Diremos que Y es subconjunto de Z, en símbolos $Y \subset Z$, si la proposición

$$a \in Y \Rightarrow a \in Z$$

es **V** cualquiera que sea $a \in X$.

Diremos que $Y = Z$ si la proposición

$$a \in Y \Leftrightarrow a \in Z$$

es verdadera. Entonces $Z = Y$ si, y sólo si, $Z \subset Y$ e $Y \subset Z$.

Sea P(x) una proposición relativa al elemento genérico x de X. Con $\{x / P(x)\}$ denotamos la totalidad de elementos de X para los cuales P(x) es **V**, o sea

$$a \in \{x / P(x)\} \text{ si, y sólo si, } P(a) \text{ es } \mathbf{V}$$

Con ϕ denotamos el subconjunto de X definido por la proposición

$$P(x) : x \in X \Rightarrow x \notin X$$

Nótese que cualquiera que sea $z \in X$

$$z \notin \phi \text{ es } \mathbf{V}$$

En efecto, si $z \in X$, entonces $z \notin X$ es **F** y así

$$z \in X \Rightarrow z \notin X \quad \text{es } \mathbf{F}$$

(por ser el antecedente **V** y el consecuente **F**). Por lo tanto

$$z \notin \{x / x \in X \Rightarrow x \notin X\} = \phi$$

Consecuentemente $\phi \subset Y$ cualquiera que sea $Y \subset X$. ϕ se denomina el conjunto vacío.

Con $\{x_1, x_2, \ldots, x_n\}$ denotamos el conjunto cuyos elementos son $x_1, x_2, \ldots, x_n$.

Sean U y V subconjuntos de X.

$$U \cup V = \{x \,/\, x \in U \;\; \text{o} \;\; x \in V\} = \text{unión de U y V.}$$
$$U \cap V = \{x \,/\, x \in U \;\cdot\; x \in V\} = \text{intersección de U y V.}$$
$$U - V = \{x \,/\, x \in U \;\cdot\; x \notin V\} = \text{diferencia de U con V.}$$
$$\mathcal{C}_x V = \mathcal{C} V = X - V = \text{complemento de V en X.}$$
$$U \,\Delta\, V = (U - V) \cup (V - U) = \text{diferencia simétrica de U y V.}$$
$$U \times V = \{(a, b) \,/\, a \in U \cdot b \in V\} = \text{producto cartesiano de U con V.}$$

Se dice que U y V son disjuntos si $U \cap V = \phi$.

Sean U, V, W subconjuntos de X. Entonces

$$U \cup (V \cup W) = (U \cup V) \cup W \text{ y escribimos simplemente}$$
$$= U \cup V \cup W$$
$$U \cap (V \cap W) = (U \cap V) \cap W \text{ y escribimos simplemente}$$
$$= U \cap V \cap W$$
$$U \cap (V \cup W) = (U \cap V) \cup (U \cap W)$$
$$U \cup (V \cap W) = (U \cup V) \cap (U \cup W)$$
$$\left.\begin{aligned} \mathcal{C}(U \cup V) &= (\mathcal{C}U) \cap (\mathcal{C}V) \\ \mathcal{C}(U \cap V) &= (\mathcal{C}U) \cup (\mathcal{C}V) \end{aligned}\right\} \text{ Leyes de De Morgan}$$
$$U \,\Delta\, (V \,\Delta\, W) = (U \,\Delta\, V) \,\Delta\, W$$
$$U \cap (V \,\Delta\, W) = (U \cap V) \,\Delta\, (U \cap W)$$

$\mathcal{P}(X)$ denota el conjunto de partes de X, o sea

$$U \in \mathcal{P}(X) \Leftrightarrow U \subset X$$

C. Aplicaciones Entre Conjuntos

Sean A y B conjuntos. Una aplicación (o función) de A en B es un subconjunto f de $A \times B$ caracterizado por

f1) Para todo $x \in A$ existe $y \in B$ tal que $(x, y) \in f$.
f2) Si $(x, y) \in f$ y $(x, y') \in f$, entonces $y = y'$.

Una aplicación de A en B está caracterizada pues por la propiedad de asignar a cada $x \in A$ un único $y \in B$.

Una aplicación f de A en B se denota por

$$f : A \to B \quad \text{o también} \quad A \xrightarrow{f} B$$

y, además, si $(x, y) \in f$ escribimos

$$f : x \to y \quad \text{o también} \quad x \to y$$
$$\text{o} \quad y = f(x)$$
$$\text{o} \quad y = fx$$

Con $id_A: A \to A$ denotamos la aplicación identidad de A:

$$id_A(x) = x \text{ cualquiera que sea } x \in A.$$

Sean $f: A \to B$ y $g: A \to B$ aplicaciones. Entonces

$f = g$ si, y sólo si, $f(x) = g(x)$ cualquiera que sea $x \in A$.

Sean A, B, C, conjuntos. Sean $g: A \to B$ y $f: B \to C$ aplicaciones. La composición de f con g es la aplicación

$$f \circ g: A \to C$$

definida por

$$f \circ g: x \to f(g(x)) \quad \text{si } x \in A$$

Si $h: C \to D$, $f: B \to C$, $g: A \to B$ entonces

$$h \circ (f \circ g) = (h \circ f) \circ g$$

y esta composición la denotamos por $h \circ f \circ g$.

Diagramas de conjuntos y aplicaciones

$$\begin{array}{ccc} & & B \\ & {}^{g}\nearrow & \downarrow f \\ A & & \\ & {}_{h}\searrow & \\ & & C \end{array} \qquad\qquad \begin{array}{ccc} A & \xrightarrow{g} & B \\ j \downarrow & & \downarrow f \\ C & \xrightarrow{h} & D \end{array}$$

se dirán conmutativos si, respectivamente,

$$h = f \circ g \quad \text{y} \quad f \circ g = h \circ j$$

Sea $f: A \to B$ una aplicación de A en B. Diremos que

f es inyectiva si $f(x) = f(x') \Rightarrow x = x'$ es **V** cualesquiera que sean $x, x' \in A$, o equivalentemente si $x \neq x' \Rightarrow f(x) \neq f(x')$ es **V** cualesquiera que sean $x, x' \in A$.

f es sobre si para todo $y \in B$ existe $x \in A$ tal que $y = f(x)$.

f es biyectiva si f es inyectiva y sobre.

Entonces $f: A \to B$ es

inyectiva si, y sólo si, existe una aplicación $g: B \to A$ tal que $g \circ f = id_A$

sobre si, y sólo si, existe una aplicación $g: B \to A$ tal que $f \circ g = id_B$

biyectiva si, y sólo si, existe una aplicación $g: B \to A$ tal que $g \circ f = id_A$ y $f \circ g = id_B$

Sea $f: A \to B$ una apliación y sea $Y \subset A$. Entonces

$$f(Y) = \{y \,/\, y \in B \text{ y existe } x \in A \text{ tal que } y = f(x)\}.$$

Los conjuntos A y B son coordinables, o A es coordinable a B si existe una aplicación $f : A \to B$ biyectiva.

D. Relaciones de Equivalencia

Sea A un conjunto. Todo subconjunto r de $A \times A$ define una relación en A por $x \sim y$ si, y sólo si, $(x, y) \in r$.

Por ejemplo, si

$$r = \{(x, y) / x = y\} = \text{Diagonal de } A$$

entonces la relación definida por r sobre A es la "igualdad". Una relación r definida sobre A se dice de equivalencia si satisface:

e1) $x \sim x$ cualquiera que sea $x \in A$.
e2) $x \sim y$ si, y sólo si, $y \sim x$.
e3) Si $x \sim z$ y $z \sim v$, entonces $x \sim v$.

Sea r una relación de equivalencia sobre A. Para todo $a \in A$ definimos

$$C_a = \{x / a \sim x\}$$

y lo denominamos la clase de equivalencia definida por a, o también la saturación de a por r.

6

Se tienen las siguientes propiedades:

- $a \in C_a$ cualquiera que sea $a \in A$
- $a \in C_b$ si, y sólo si, $b \in C_a$
- $C_a = C_b$ si, y sólo si, $a \sim b$
- $C_a \cap C_b = \phi$ ó $C_a = C_b$

Se denomina conjunto cociente de A por r y se le denota por A/r, o también $A/\sim$, al conjunto formado por todas las clases de equivalencia de elementos de A:

$$A/\sim = \{C_a / a \in A\}$$

Se denomina aplicación canónica de A en $A/\sim$ a la aplicación

$$g : A \to A/\sim$$

definida por

$$g(a) = C_a$$

g es una aplicación sobre.

Ejemplo

Sea $A = \{1, -1, 2\}$. Entonces $x \sim y$ si, y sólo si, $x^2 = y^2$ es una relación de equivalencia sobre A. Se tiene

$$C_1 = C_{-1} = \{1, -1\} \quad C_2 = \{2\}$$

$g : A \to A/\sim$ está dada por

$$g(1) = g(-1) = \{1, -1\}$$
$$g(2) = \{2\}$$

E. Aritmética

Conjuntos numéricos:

$\mathbf{N}$ = conjunto de los números naturales
$\mathbf{Z}$ = conjunto de los números enteros
$\mathbf{Q}$ = conjunto de los números racionales
$\mathbf{R}$ = conjunto de los números reales
$\mathbf{C}$ = conjunto de los números complejos

$m \in \mathbf{Z}$ si, y sólo si, $m = 0$ o $m \in \mathbf{N}$ o $-m \in \mathbf{N}$.
$m \in \mathbf{Q}$ si, y sólo si, existen enteros r, s, $s \neq 0$ tales que $m = r \cdot s^{-1} = r/s$.

Principio de Inducción. Sea H un subconjunto de $\mathbf{N}$ tal que

i. $1 \in H$
ii. Si $m \in H$ entonces $m + 1 \in \mathbf{N}$
Entonces $H = \mathbf{N}$

Algoritmo de División. Sean m y n enteros, $0 < n$. Existen enteros q y r que satisfacen

a) $m = n \cdot q + r$
b) $0 \leq r < n$

Si además q' y r' son enteros que satisfacen a) y b) se tiene $q = q'$ y $r = r'$.

Sean m y n enteros no nulos. Diremos que n divide a m, o que n es divisor de m, o que m es múltiplo de n, .. si existe $c \in \mathbf{Z}$ tal que $m = n \cdot c$. Escribimos n / m. Entonces si n/m y m/r se tiene n/r, $n, m, r \in \mathbf{Z}$. Se denominan divisores triviales de un entero m a los enteros $1, -1, m, -m$. Un entero positivo $p \neq 1$ se dice primo si sus únicos divisores son triviales.

Se denomina máximo común divisor de m y n a todo entero positivo d que satisface

M1) d/m y d/n
M2) si $d' \in \mathbf{N}$ satisface d'/m y d'/n entonces d'/d.

El máximo común divisor de m y n existe y es único, y se lo denota por (n, m). Se tiene además la siguiente relación: existen enteros a y b tales que

$$(n, m) = n \cdot a + m \cdot b$$

Si $(n, m) = 1$ se dice que n y m son coprimos.

Se denomina mínimo común múltiplo de m y n a todo entero positivo t que satisface

m1) n/t y m/t
m2) si $t' \in \mathbf{N}$ satisface n/t' y m/t' entonces t/t'.

El mínimo común múltiplo de n y m existe y es único y se lo denota por $[n, m]$. Se tiene la igualdad

$$n \cdot m = (n, m) \cdot [n, m]$$

Sea $m \in \mathbf{N}$. La relación en $\mathbf{Z}$:

$$a \sim b \text{ si, y sólo si, } m/(a - b)$$

es una relación de equivalencia, que se denomina la congruencia módulo m y se denota por $a \equiv b \mod (m)$.

Sea en $\mathbf{Z}$ la relación $\leq$ de orden menor o igual. Llamaremos sección a la derecha de $\mathbf{Z}$ a todo subconjunto de $\mathbf{Z}$ de la forma

$$S_a = \{x / a \leq x\}$$

Principio de Buena Ordenación. Toda sección a la derecha S_a de $\mathbf{Z}$ satisface la siguiente propiedad:

Si $H \subset S_a$ y $\emptyset \neq H$ existe $h_0 \in H$ tal que $h_0 \leq h$ cualquiera que sea $h \in H$. O sea, todo subconjunto no vacío de H posee primer elemento.

Este Principio de Buena Ordenación es equivalente al Principio de Inducción en $\mathbf{N}$. Aquí lo aplicaremos a la sección S_0 de $\mathbf{Z}$.

I. ESTRUCTURAS DE MONOIDE Y SEMIGRUPO

A. Leyes de Composición

Definición. Sea A un conjunto no vacío. Llamaremos ley de composición interna (o simplemente ley de composición) definida sobre A a toda aplicación:

$$* : A \times A \to A$$

Si $x, y \in A$ escribimos

$$*(x, y) = x * y$$

Al elemento $x * y$ lo denominamos la composicion (por $*$) de x con y.

La definición anterior formaliza la noción de operación binaria entre elementos de A. Las operaciones de suma y producto entre números constituyen los ejemplos naturales de leyes de composición.

Definición. Se llama MONOIDE a todo par $(A, *)$ formado por un conjunto A y una ley de composición $*$. Diremos también que $*$ define sobre A una estructura de monoide.

Obsérvese que a veces se sobreentenderá la ley de composición $*$ definida sobre A y se denotará $(A, *)$ simplemente por A, y nos referiremos al monoide A.

Por ejemplo, si A denota cualquiera de los conjuntos numéricos

$$\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$$

y $*$ la suma ordinaria $+$ o el producto ordinario $\cdot$ de números, se obtienen los siguientes monoides:

$$(\mathbf{N}, +), \quad (\mathbf{N}, \cdot)$$
$$(\mathbf{Z}, +), \quad (\mathbf{Z}, \cdot)$$
$$(\mathbf{Q}, +), \quad (\mathbf{Q}, \cdot)$$
$$(\mathbf{R}, +), \quad (\mathbf{R}, \cdot)$$
$$(\mathbf{C}, +), \quad (\mathbf{C}, \cdot)$$

Veamos otros ejemplos:

1. $A = \mathbf{N}$
   $x * y = (x, y) =$ máximo común divisor de x e y

2. $A = \mathbf{N}$
   $x * y = [x, y] =$ mínimo común múltiplo de x e y

3. $A = \mathbf{Z}$
   $x * y = 0$

4. $A = \mathbb{Z}$
$x * y = x - y$ (- denota la diferencia de enteros)

5. $A = \mathbb{Z}$
$x * y = x^2 \cdot y^2$ (· denota el producto ordinario de enteros)

6. $A = \mathbb{Z}$
$x * y = x$

Sea X un conjunto y sea $A = \mathcal{P}(X)$ el conjunto de partes de X. Entonces las siguientes estructuras de monoides pueden considerarse sobre A

7. $A = \mathcal{P}(X)$
$U * V = U \cup V$

8. $A = \mathcal{P}(X)$
$U * V = U \cap V$

9. $A = \mathcal{P}(X)$
$U * V = U - V$

10. $A = \mathcal{P}(X)$
$U * V = U \Delta V$

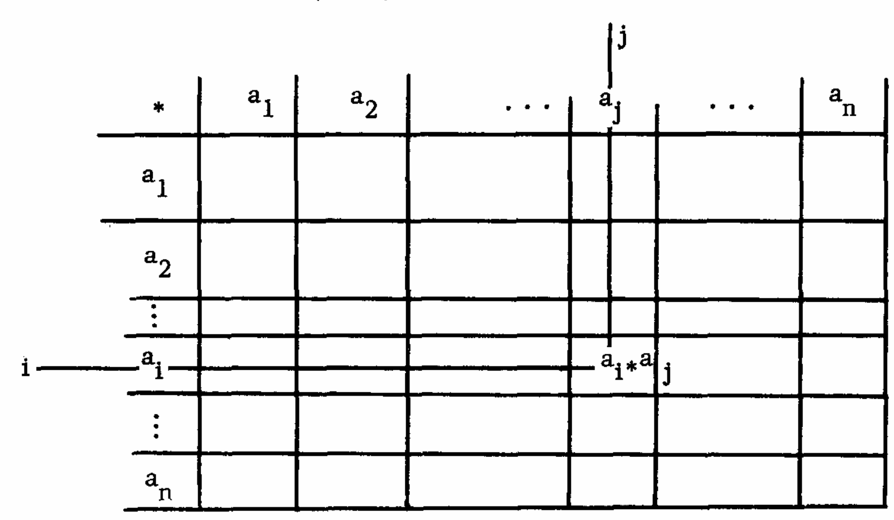
Otra categoría importante de monoides la constituyen los llamados monoides finitos.

Definición. Diremos que un monoide (A, *) es finito si el conjunto A es finito. En todo otro caso diremos que (A, *) es infinito.

La descripción de los monoides finitos se hace mediante tablas de composición. Por ejemplo, si

$$A = \{a_1, \ldots, a_n\}$$

construimos la tabla (de *)



escribiendo en la casilla ubicada en la intersección de la fila i y la columna j, el elemento $a_i * a_j$.

Algunos ejemplos son:

11. $A = \{0, 1, 2\}$

*	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

es el monoide definido por

$0 * 0 = 0$	$0 * 1 = 1$	$0 * 2 = 2$
$1 * 0 = 1$	$1 * 1 = 2$	$1 * 2 = 0$
$2 * 0 = 2$	$2 * 1 = 0$	$2 * 2 = 1$

12. $A = \{0, 1, 2\}$

*	0	1	2
0	0	0	0
1	1	1	1
2	2	2	2

es el monoide definido por

$$x * y = x$$

Ejercicio. Sea A un conjunto finito de n elementos. ¿Cuál es el número máximo de estructuras de monoide que pueden denifirse sobre A? Hallar todas las estructuras de monoide para el caso $n = 2$.

B. Composiciones n-arias. Asociatividad

Sea $(A, *)$ un monoide. Las composiciones

$$x * y \in A$$

si $x, y \in A$ constituyen las composiciones binarias de elementos de A. Si x, y, z denotan elementos de A dados en un cierto orden, podemos obtener los siguientes elementos de A "vía" composiciones binarias:

$$x * (y * z)$$
$$(x * y) * z$$

Análogamente, con elementos x, y, z, v de A, dados en un cierto orden, podemos formar los siguientes elementos de A "vía" composiciones binarias:

$$a = x * (y * (z * v)) \qquad b = x * ((y * z) * v)$$

$$\text{(I)} \qquad c = (x * y) * (z * v)$$

$$d = (x * (y * z)) * z \qquad e = ((x * y) * z) * z$$

(¿Descubre el lector la ley de formación?)

En general, dados n elementos $x_1, x_2, .., x_n$ de A en un cierto orden, llamaremos composición n-aria de los mismos a todo elemento de A que se obtenga de $x_1, x_2, .., x_n$ por sucesivas composiciones binarias, conservando siempre el orden inicial.

Las composiciones n-arias no tienen porque ser necesariamente iguales entre sí. Por ejemplo, en el monoide (**Z**, -) de enteros racionales, con la diferencia como ley de composición, existen elementos x, y, z en **Z** cuyas composiciones ternarias no coinciden. En efecto, sean

$$x = y = z = 1$$

Entonces

$$x * (y * z) = x - (y - z) = 1 - (1 - 1) = 1$$
$$(x * y) * z = (x - y) - z = (1 - 1) - 1 = -1$$

Definición. Sea (A, *) un monoide y sea $n \in$ **N**, $2 < n$. Diremos que * es <u>n-asociativa</u> si cualesquiera que sean $x_1, x_2, .., x_n$ en A, dados en un cierto orden, coinciden entre sí todas sus composiciones n-arias. Diremos que * es <u>asociativa</u> si es n-asociativa, cualquiera que sea n.

Definición. Se denomina SEMIGRUPO a todo monoide cuya ley de composición es asociativa.

Teorema. Un monoide (A, *) es un semigrupo si, y sólo si, * es 3-asociativa, o sea si, y sólo si,

$$x * (y * z) = (x * y) * z$$

cualesquiera que sean x, y, z en A. En otros términos, una ley de composición es asociativa si, y sólo si, es 3-asociativa.

Demostración. Si (A, *) es un semigrupo, entonces * es n-asociativa para todo n, y lo será en particular si n = 3, de manera que la parte "sólo si" del teorema queda probada. Veamos la parte "si". Vamos a probar que 3-asociatividad implica n-asociatividad cualquiera que sea n. Antes de continuar ilustremos un caso particular de esta implicación, a saber: 3-asociatividad implica 4-asociatividad. O sea, debemos probar que todos los elementos a, b, c, d, e de (I)

coinciden entre sí. Para ello compararemos todas las composiciones cuaternarias con la composición a:

$$\begin{aligned}
b &= x * ((y * z) * v) = x * (y * (z * v)) = a \\
c &= (x * y) * (z * v) = x * (y * (z * v)) = a \\
d &= (x * (y * z)) * v = ((x * y) * z) * v \\
&\qquad\qquad\qquad\quad = (x * y) * (z * v) = c = a \\
e &= ((x * y) * z) * v = (x * (y * z)) * v = d = a
\end{aligned}$$

por lo tanto

$$a = b = c = d = e$$

Para la demostración general, siguiendo el esquema anterior, individualizaremos, para cada conjunto finito

$$x_1, x_2, \ldots, x_n$$

la composición n-aria

$$x_1 * (x_2 * (\ldots . (x_{n-1} * x_n) \ldots .))$$

que denominaremos la composición n-aria principal. Así, por ejemplo, para $n = 3$

$$x_1 * (x_2 * x_3)$$

para $n = 4$

$$x_1 * (x_2 * (x_3 * x_4))$$

para $n = 5$

$$x_1 * (x_2 * (x_3 * (x_4 * x_5)))$$

Procederemos por inducción en n. El caso $n = 3$ es verdadero por hipótesis. Sea válida la k-asociatividad para todo $k < n$. Sean $x_1, x_2, \ldots, x_n$ elementos de A, dados en un cierto orden, y sea $3 < n$. Sea x una composición n-aria de $x_1, x_2, \ldots, x_n$. Entonces x es, en última instancia, una composición binaria

$$x = a_1 * a_2$$

donde

$a_1 = x_1$ o $a_1 =$ una composición k-aria de $x_1, \ldots, x_k$, $1 < k$
$a_2 = x_n$ o $a_2 =$ una composición $(n - k)$-aria de $x_{k+1}, \ldots, x_n$

Por la hipótesis inductiva se tiene

$a_1 = x_1$ o $a_1 = x_1 * (x_2 * \ldots (x_{k-1} * x_k) \ldots) =$ la composición k-aria principal asociada a $x_1, \ldots, x_k$
$= x_1 * a_1'$ siendo $a_1' = (x_2 * \ldots (x_{k-1} * x_k) \ldots)$

Por lo tanto

$$x = a_1 * a_2 = (x_1 * a_1') * a_2 = x_1 * (a_1' * a_2)$$

y siendo $a_1' * a_2$ una composición (n - 1)-aria debe coincidir con la composición (n - 1)-aria principal asociada a $x_2, \ldots, x_n$. En consecuencia

$$x = x_1 * (x_2 * (\ldots (x_{n-1} * x_n) \ldots))$$

Queda entonces probada la n-asociatividad. En virtud del Principio de Inducción se tiene n-asociatividad para todo n y, por tanto, asociatividad, que es lo que queríamos probar.

En virtud del teorema anterior, tratándose de un semigrupo, denotaremos con

$$x_1 * x_2 * \ldots * x_n$$

la (única) composición n-aria de elementos $x_1, \ldots, x_n$ de A, dados en ese orden. En particular

$$x * y * z = x * (y * z) = (x * y) * z$$

Un caso importante es aquél en que

$$x_1 = x_2 = \ldots = x_n = x$$

escribimos

$$x_1 * \ldots * x_n = x^n$$

A manera de ejercicio dejamos a cargo del lector verificar las siguientes relaciones:

$$x^n * x^m = x^{n+m} \quad \text{y} \quad (x^n)^m = x^{n \cdot m}$$

cualesquiera que sean $n, m \in \mathbf{N}$.

Ejemplos

1. Los monoides numéricos considerados anteriormente $(\mathbf{N}, +)$, $(\mathbf{N}, \cdot), \ldots, (\mathbf{C}, \cdot)$ son todos semigrupos.

2. El monoide $(\mathbf{N}, *)$, donde $x * y = (x, y)$ = máximo común divisor de x e y, es un semigrupo. En efecto, recordemos la definición de (x, y):

i. $(x, y) \in \mathbf{N}$
ii. (x, y) divide a x y divide a y
iii. Si $d \in \mathbf{N}$ satisface "d divide a x y d divide a y" entonces "d divide a (x, y)".

Vamos a probar entonces que cualesquiera que sean $x, y, z \in \mathbf{N}$ es válido

$$(x, (y, z)) = ((x, y), z)$$

Llamemos d_1 al término de la izquierda y d_2 al término de la derecha. Entonces, en virtud de ii

$$d_1 \text{ divide a } x \text{ y } d_1 \text{ divide a } (y, z)$$

por lo tanto

$$d_1 \text{ divide a } x, \quad d_1 \text{ divide a } y, \quad d_1 \text{ divide a } z$$

Ahora en virtud de iii

$$d_1 \text{ divide a } (x, y)$$

o sea

$$d_1 \text{ divide a } (x, y) \text{ y } d_1 \text{ divide a } z$$

Se sigue de iii que

$$d_1 \text{ divide a } ((x, y), z) = d_2$$

Queda pues probado que d_1 divide a d_2. Razonando en forma análoga para el caso simétrico, se obtendría que d_2 divide a d_1. Pero entonces reuniendo estas dos afirmaciones resulta

$$d_1 = d_2$$

que es lo que queríamos demostrar.

3. $(\mathbf{N}, *)$, donde $x * y = [x, y]$ = mínimo común múltiplo de x e y, es un semigrupo. La demostración es análoga a la precedente.

4. Sea X un conjunto no vacío y sea $A = \text{Aplc}(X)$ la totalidad de aplicaciones de X en X. Entonces, si $f, g \in A$ podemos definir la aplicación $f \circ g : X \to X$ composición de f con g por

$$x \to f(g(x))$$

por lo tanto $(\text{Aplc}(X), \circ)$ es un monoide. Sean ahora $f, g, h \in A$. Si $x \in X$ resulta

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$$
$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$

de manera que

$$(f \circ g) \circ h = f \circ (g \circ h)$$

o sea $(\text{Aplc}(X), \circ)$ es un semigrupo: <u>el semigrupo de aplicaciones de X.</u>

<u>Ejercicios</u>

1. Encontrar todas las estructuras de semigrupo que pueden definirse en $A = \{0, 1\}$.

2. Determinar en los monoides siguientes cuáles son semigrupos:

   a) $(\mathbf{Z}, *)$ donde $x * y = x + y + x \cdot y$
   b) $(\mathbf{Z}, *)$ donde $x * y = x^2 - y^2$
   c) $(\mathbf{Z}, *)$ donde $x * y = x$
   d) $(\mathbf{Z}, *)$ donde $x * y = x + 1$

3. Verificar si el siguiente monoide es o no semigrupo

*	a	b	c
a	a	b	c
b	b	b	b
c	c	c	c

C. **Conmutatividad**

Sea (A, *) un monoide.

Definición. Diremos que $x, y \in A$ conmutan entre sí si

$$x * y = y * x$$

Diremos que (A, *) es un monoide conmutativo (o también que * es conmutativa) si todo par de elementos de A conmutan entre sí.

Obsérvese que en todo monoide existen pares de elementos que conmutan entre sí: en efecto, $x * x = x * x$. Si (A, *) es un semigrupo entonces cualesquiera que sean $n, m \in N$ y $x \in A$:

$$x^n * x^m = x^{n+m} = x^m * x^n$$

Sea (A· *) un semigrupo conmutativo. Entonces si $x_1, x_2, x_3 \in A$ valen las relaciones:

$$(1)\quad \begin{aligned} x_1 * x_2 * x_3 &= x_2 * x_1 * x_3 = x_2 * x_3 * x_1 = x_3 * x_2 * x_1 \\ &= x_3 * x_1 * x_2 = x_1 * x_3 * x_2 \end{aligned}$$

Cada expresión en las relaciones precedentes está evidentemente caracterizada por los subíndices 1, 2 y 3 considerados en un cierto orden. Es decir, cada expresión está caracterizada por una "permutación" del conjunto $\{1, 2, 3\}$. Por tanto, si s denota una permutación del conjunto $\{1, 2, 3\}$ las relaciones (1) pueden escribirse

$$x_1 * x_2 * x_3 = x_{s(1)} * x_{s(2)} * x_{s(3)}$$

En general dados

$$x_1, \ldots, x_n$$

pertenecientes a un semigrupo conmutativo, se tiene que cualquiera que sea la permutación s del conjunto $\{1, 2, \ldots, n\}$

$$x_1 * x_2 * \ldots * x_n = x_{s(1)} * x_{s(2)} * \ldots * x_{s(n)}$$

o también utilizando el signo de producto π

$$\prod_{i=1}^{n} x_i = \prod_{i=1}^{n} x_{s(i)}$$

Una relación importante válida en semigrupos conmutativos es la siguiente: cualesquiera que sean x, y $\in$ A y n $\in$ **N**:

(2) $$(x * y)^n = x^n * y^n$$

Por ejemplo, en el caso n = 2, su demostración es la siguiente:

$$\begin{aligned}(x * y)^2 &= (x * y) * (x * y) = \\ &= x * (y * x) * y \\ &= x * (x * y) * y \\ &= (x * x) * (y * y) \\ &= x^2 * y^2\end{aligned}$$

La demostración general de (2) se realiza por inducción en n. Ya la hemos demostrado para n = 2. Sea n > 2. Entonces

$$\begin{aligned}(x * y)^n &= (x * y)^{n-1} * (x * y) \\ &= (x^{n-1} * y^{n-1}) * (x * y) \quad \text{(por hipótesis inductiva)} \\ &= x^{n-1} * (y^{n-1} * x) * y \\ &= x^{n-1} * (x * y^{n-1}) * y \\ &= (x^{n-1} * x) * (y^{n-1} * y) \\ &= x^n * y^n\end{aligned}$$

Obsérvese que para la demostración de (2) sólo se utiliza la asociatividad de * y el hecho de que x e y conmutan entre sí. Por tanto (2) es válida en todo semigrupo y para todo par de elementos del mismo que conmutan entre sí.

Ejemplo. Sea (**N**, *) el semigrupo definido por x * y = x. Entonces, si x, y $\in$ **N** y n $\in$ **N**

$$(x * y)^n = x^n$$
$$x^n * y^n = x^n$$

Por tanto

$$(x * y)^n = x^n * y^n$$

y sin embargo si $x \neq y$

$$x * y \neq y * x$$

Se sigue entonces que (2) no es equivalente a la conmutatividad de x e y, o sea

$$x * y = y * x \Rightarrow (x * y)^n = x^n * y^n$$
cualquiera que sea n $\in$ **N**

siendo falsa la implicación recíproca.

D. Identidades e Inversos

Sea (A, *) un monoide. Resulta natural estudiar la existencia en A de elementos que gozan de las propiedades análogas al 0 en el

monoide $(\mathbf{Z}, +)$ y al 1 en el monoide $(\mathbf{N}, \cdot)$, a saber

$$m + 0 = 0 + m = m \quad \text{cualquiera que sea } m \in \mathbf{Z}$$
$$n \cdot 1 = 1 \cdot n = n \quad \text{cualquiera que sea } n \in \mathbf{N}$$

Entonces

Definición. Se dice que un elemento $e \in A$ es

i. identidad a la izquierda de $*$ si

$$e * a = a$$

cualquiera que sea $a \in A$

ii. identidad a la derecha de $*$ si

$$a * e = a$$

cualquiera que sea $a \in A$

iii. identidad de $*$ si es simultánea la identidad a la izquierda y a la derecha de $*$.

Es claro que en el caso de monoides conmutativos no es necesario hacer distinciones entre identidad a la izquierda y a la derecha. Antes de dar algunos ejemplos anotemos la siguiente proposición.

Proposición. Sea $(A, *)$ un monoide. Sean e_1, $e_2 \in A$. Entonces,
si e_1 es identidad a la izquierda de $*$ y
si e_2 es identidad a la derecha de $*$, se tiene

$$e_1 = e_2$$

Demostración. Por hipótesis

$$e_1 * a = a$$
$$b * e_2 = b$$

cualesquiera que sean a y $b \in A$. En particular si $a = e_2$ y $b = e_1$ resulta

$$e_2 = e_1 * e_2 = e_1$$

Corolario. En todo monoide existe a lo sumo una identidad.

Corolario. Si un monoide no posee identidad pero posee identidad a la izquierda (respectivamente a la derecha) entonces no posee ninguna identidad a la derecha (respectivamente a la izquierda).

Corolario. Si un monoide posee identidad entonces posee una única identidad a la izquierda y una única identidad a la derecha.

Ilustremos con algunos ejemplos.

Ejemplos

1. (**N**, *) donde x * y = x. Todo elemento de N es identidad a la derecha, pero no existe identidad a la izquierda.

2. (**N**, *) donde x * y = (x, y) = máximo común divisor de x e y. No posee elemento de identidad.

3. (**N**, *) donde x * y = [x, y] = mínimo común múltiplo de x e y. 1 es elemento identidad.

4. (**Z**, *) donde x * y = x - y. 0 es identidad a la derecha. No posee identidad a la izquierda.

5. Sea X un conjunto y sea (Aplc(X), o) el semigrupo de aplicaciones de X. La aplicación identidad id_A: X → X, definida por

$$id_A(x) = x$$

cualquiera que sea x ε X, es elemento identidad de (Aplc(X), o).

Notación. Se denotará con (A, *, e) un monoide con elemento identidad e.

Definición. Sea (A, *, e) un monoide con identidad. Sea a ε A. Diremos que

i. posee un inverso a la izquierda (respecto de e) si existe b ε A tal que

$$b * a = e$$

ii. posee un inverso a la derecha (respecto de e) si existe c ε A tal que

$$a * c = e$$

iii. posee un inverso (respecto de e), o que es inversible, si existe d ε A tal que

$$d * a = a * d = e$$

Ejemplos

1. En (**N**, ., 1) el único elemento con inverso es el 1.

2. En (**Z**, ., 1) los únicos elementos con inverso son 1 y -1.

3. En (**Q**, ., 1) todo elemento distinto de 0 posee un inverso.

4. En el monoide cuya tabla de composición es

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	1	2	0	2
3	2	3	1	1

i. poseen inverso a la izquierda:

$$\begin{array}{lcl} 0 & : & 2 * 0 = 1 \\ 1 & : & 1 * 1 = 1 \\ 2 & : & 3 * 2 = 1 \\ 3 & : & 3 * 3 = 1 \end{array}$$

ii. poseen inverso a la derecha:

$$\begin{array}{lcl} 1 & : & 1 * 1 = 1 \\ 2 & : & 2 * 0 = 1 \\ 3 & : & 3 * 2 = 3 * 3 = 1 \end{array}$$

iii. poseen inverso:

$$\begin{array}{lcl} 1 & : & 1 * 1 = 1 * 1 = 1 \\ 3 & : & 3 * 3 = 3 * 3 = 1 \end{array}$$

El ejemplo 4 sugiere todo tipo de anomalías en cuanto a la existencia de inversos (a la izquierda, a la derecha). Observemos, sin embargo, que dicho monoide no es asociativo. En el caso asociativo la situación es más regular, según lo indica la siguiente proposición.

Proposición. Sea $(A, *, e)$ un semigrupo. Entonces si $a \in A$ posee un inverso a la izquierda b y un inverso a la derecha c, se verifica

$$b = c$$

Demostración

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c$$

En virtud de la unicidad dada en la proposición anterior se adopta:

Notación. Sea $(A, *, e)$ un semigrupo con identidad. Si $a \in A$ posee un inverso b en A, escribiremos $a' = b$.

Ejemplo. Sea $(\text{Aplc}(\mathbf{N}), \text{o}, id_{\mathbf{N}})$ el semigrupo de aplicaciones del conjunto de números naturales. Sea $f \in \text{Aplc}(\mathbf{N})$ definida por

$$f(n) = 2n \text{ si } n \in \mathbf{N}$$

Sea $g \in \text{Aplc}(\mathbf{N})$ definida por

$$g(n) = \begin{cases} n/2 & \text{si } n \text{ es par} \\ (n+1)/2 & \text{si } n \text{ es impar} \end{cases}$$

Es fácil entonces verificar que

$$g \text{ o } f = id_{\mathbf{N}}$$

de manera que g es inverso a la izquierda de f. Sin embargo, f no posee ningún inverso a la derecha. En efecto, de existir un inverso h a la derecha de f, se tendría $g = h$, según la proposición anterior.

Pero entonces f sería biyectiva, lo cual no es así. Es fácil ver también que f posee infinitos inversos a la izquierda, todos distintos entre sí.

Proposición. Sea $(A, *, e)$ un semigrupo con identidad.

1. si $u \in A$ posee un inverso a la izquierda $v \in A$ y si $x \in A$ posee un inverso a la izquierda $y \in A$, entonces $v * y$ es un inverso a la izquierda de $x * u$.
2. Idéntica proposición con inversos a la derecha.
3. Si x' es un inverso de x y si u' es un inverso de u, entonces $x * u$ es inversible en A y se tiene

$$\boxed{(x * u)' = u' * x'}$$

Demostración. Será suficiente probar 1 dado que 2 es de demostración análoga y 3 es consecuencia de 1 y 2.

Se tiene por hipótesis

$$v * u = e$$
$$y * x = e$$

por lo tanto

$$\begin{aligned}(v * y) * (x * u) &= v * (y * x) * u \\ &= v * e * u = v * u \\ &= e\end{aligned}$$

conforme queríamos probar.

Razonando inductivamente se tiene:

Corolario. Sea $(A, *, e)$ un semigrupo con identidad. Sean $x_1, x_2, \ldots, x_n$ elementos de A con inversos en A $x_1', x_2', \ldots x_n'$, respectivamente. Entonces $x_1 . x_2 . . x_n$ es inversible en A y

$$(x_1 . x_2 . . . x_n)' = x_n' . . . x_2' . x_1'$$

Proposición. Sea $(A, *, e)$ un semigrupo con identidad. Si $x \in A$ es inversible, entonces su inverso x' también es inversible y satisface

$$\boxed{(x')' = x}$$

Demostración. Se sigue de la interpretación de las igualdades

$$x * x' = x' * x = e$$

en términos de la definición de inverso.

E. Submonoides

Un procedimiento natural en el estudio de una estructura algebraica es el de investigar las estructuras "más pequeñas" de la misma o, más propiamente dicho, las llamadas subestructuras. En

muchos casos el conocimiento de cierta familia de subestructuras permite una descripción de la estructura de partida (a manera de ejemplo, para el lector informado, los grupos abelianos finitos están completamente determinados por el conocimiento de ciertos de sus subgrupos "cíclicos"). En este sentido definiremos en esta sección submonoide y subsemigrupo.

Definición. Sea (A, *) un monoide. Sea C un subconjunto de A. Diremos que * define sobre C una estructura de submonoide, o también simplemente que C es submonoide de A, si se satisfacen las dos condiciones siguientes:

i. $C \neq \phi$
ii. $x, y \in C \Rightarrow x * y \in C$.

Definición. Sea (A, *) un monoide. Sea C un subconjunto de A. Diremos que * define sobre C una estructura de subsemigrupo, ó simplemente que C es un subsemigrupo de A, si se satisfacen las dos condiciones siguientes:

i. C es submonoide de A
ii. * es asociativa sobre C, o sea

$$x * (y * z) = (x * y) * z$$

cualesquiera que sean x, y, z en C!.

Si C es submonoide de un monoide (A, *), entonces la restricción de * a C define sobre C una estructura de monoide, de manera que todo submonoide es, en forma natural, un monoide. Análogamente, un subsemigrupo de un monoide es, en forma natural, un semigrupo.

Ejercicio. Probar que todo submonoide de un semigrupo es semigrupo.

Antes de entrar a la consideración de ejemplos específicos, observemos que todo monoide (A, *) posee siempre un submonoide, a saber, el mismo A.

Ejemplos

1. Sea $(\mathbf{Z}, *)$ donde $x * y = x - y$. Entonces:
   a) $C = \{0\}$
   b) $C \quad \{.., -4, -2, 0, 2, 4, ..\} = \{2m \,/\, m \in \mathbf{Z}\}$

son submonoides de $(\mathbf{Z}, *)$; a) es subsemigrupo, pero b) no lo es. La parte a) admite la siguiente generalización: sea A un monoide y sea $a \in A$ un elemento idempotente, o sea tal que $a^2 = a * a = a$. Entonces $\{a\}$ es un subsemigrupo de A.

2. Sea (A, *) donde $A = \{0, 1, 2\}$ y donde $x * y = x$. Entonces todo subconjunto no vacío de A es un submonoide de A.

3. Sea (A, *) dado por la tabla

*	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

entonces

$$C = \{0\} \quad \text{y} \quad C = \{0, 1, 2\}$$

son los únicos submonoides de A.

4. Sean X un conjunto e $Y \subset X$ un subconjunto. Sea $A = \mathcal{P}(X)$ el conjunto de partes de X. Sea (A, *) el monoide definido por

$$u * v = u \cap v$$
$$u \subset X, \; v \subset X$$

$C = \mathcal{P}(Y) \subset \mathcal{P}(X)$ es submonoide de (A, *). Obsérvese en este ejemplo que

X es identidad de (A, *) (en efecto, $u \cap X = u$)

$Y \neq X \Rightarrow X \notin C$

por tanto, un submonoide no "hereda" necesariamente la identidad del monoide, si éste último posee una.

5. Sea (A, *) un semigrupo y sea $a \in A$ un elemento que fijamos de antemano. Sea

$$C_a = \{a^k / k \in \mathbf{N}\}$$

el conjunto de todas las potencias naturales de a. Las relaciones

$$a^k * a^j = a^{k+j}$$

y el hecho de ser $C_a \neq \emptyset$ muestran que C_a es submonoide de A. Este submonoide tiene la propiedad: si C es submonoide de A y además $a \in C$, entonces $C_a \subset C$. En este sentido C_a es el menor submonoide de A que contiene a y se le denomina el submonoide engendrado por a. Ilustremos especializando A y a.

i. $(A, *) = (\mathbf{N}, +)$. Notemos que

$$a^2 = a * a = a + a = 2a$$
$$a^3 = a * a * a = a + a + a = 3a$$

Entonces

$$C_1 = \{1, 2, 3, \ldots\} = \mathbf{N}$$
$$C_2 = \{2, 4, 6, \ldots\}$$

ii. $(A, *) = (\mathbf{N}, .)$

$$C_1 = \{1\}$$
$$C_2 = \{2, 4, 8, 16, 32, \ldots\}$$
$$C_3 = \{3, 9, 27, 81, \ldots\}$$

iii. $(A, *) = (\mathbf{Z}, .)$

$$C_{-1} = \{-1, 1\}$$

6. Sea $(A, *, e)$ un semigrupo con identidad. Sea $U(A)$ la totalidad de elementos inversibles de A. (La razón de utilizar $U(A)$ se debe a que los elementos inversibles suelen llamarse también unidades de A.) Nuestra afirmación es: $U(A)$ es un subsemigrupo de A. En efecto, $U(A) \neq \emptyset$ dado que $e \in U(A)$. La relación

$$v' * u' = (u * v)'$$

nos dice que

$$u, v \in U(A) \Rightarrow u * v \in U(A)$$

Puesto que la asociatividad de $*$ sobre $U(A)$ es consecuencia de la asociatividad de $*$ en A, se tiene que $U(A)$ es un subsemigrupo de A: el subsemigrupo de elementos inversibles de A (o también el subsemigrupo de unidades de A).

Particularicemos A.

a) Sea X un conjunto no vacío y sea $Aplc(X) = A$ el semigrupo de aplicaciones de X. Entonces

$$\begin{aligned} f \in U(Aplc(X)) &\Leftrightarrow \text{Existe } g \in Aplc(X) \text{ tal que } \\ &\quad\; f \circ g = g \circ f = id_x \\ &\Leftrightarrow f \text{ es biyectiva} \end{aligned}$$

Por lo tanto, $U(A)$ coincide con la totalidad de aplicaciones biyectivas de X en X, o sea con las transformaciones de X. Escribimos

$$\boxed{U(Aplc(X)) = Tran(X)}$$

y lo denominamos el semigrupo de transformaciones de X.

b) Sea $A = (\mathbf{Z}, ., 1)$. Entonces $U(A) = \{1, -1\}$.

c) Sea $A = (\mathbf{N}, ., 1)$. Entonces $U(A) = \{1\}$.

d) $A = \{1, 2, 3, 6\}$ con $x * y = (x, y)$ = máximo común divisor de x e y. Entonces $U(A) = \{6\}$.

e) Sea $A = (\mathbf{Z}, +, 0)$. Entonces $U(A) = \mathbf{Z}$.

F. Morfismos

El modo natural en matemática de vincular dos conjuntos A y B es mediante aplicaciones de A en B o viceversa. Por supuesto que más que conjuntos lo que interesa es relacionar las propiedades que poseen los mismos y, por tanto, las aplicaciones de uno en otro deben también relacionar las propiedades en cuestión. En nuestro estudio, por ejemplo, los conjuntos poseen leyes de composición.

Si intentamos establecer una relación entre dos de tales conjuntos debemos entonces buscar que las aplicaciones "respeten" esas leyes de composición. Por ejemplo, los conjuntos **N** y **Z** de números naturales y de enteros poseen ambos la propiedad conjuntista de ser coordinables entre sí, o sea que existe una aplicación biyectiva

(1) $$f : \mathbf{Z} \to \mathbf{N}$$

Ahora en **N** y **Z** hay, en ambos casos, leyes de composición como, por ejemplo, la suma. Sin embargo, no existe ninguna aplicación biyectiva (1) que preserve dichas leyes de composición, o sea que no existe una aplicación biyectiva $f : \mathbf{Z} \to \mathbf{N}$ tal que

(2) $$f(m + n) = f(m) + f(n)$$

Las razones son muy sencillas, ya que de existir una tal aplicación se verificaría lo siguiente:

(3) $$f(m) = f(m + 0) = f(m) + f(0)$$

pero tratándose de números naturales

$$f(m) \neq f(m) + f(0)$$

de manera que (3) es un absurdo, consecuencia de suponer la existencia de una aplicación $f : \mathbf{Z} \to \mathbf{N}$ con la propiedad de preservar las "sumas". Note el lector que en realidad la condición de ser f biyectiva no es necesaria, por lo que, en definitiva, hemos probado que no existe ninguna aplicación $f : \mathbf{Z} \to \mathbf{N}$ que preserve las sumas en sentido de (2).

Formalicemos ahora la discusión anterior: sean (A, *) y (B, *) monoides.

Definición. Se denomina morfismo o también homomorfismo de (A, *) en (B, *), o simplemente de A en B, a toda aplicación $f : A \to B$ que satisfaga:

$$f(x * y) = f(x) * f(y)$$

cualesquiera que sean $x, y \in A$.

Además, si A y B poseen elementos identidad (que denotamos en ambos casos por e) f satisface

$$f(e) = e$$

Un morfismo de A en A se denomina también endomorfismo de A.

Veamos algunas propiedades de morfismos y, por razones de simplicidad, supongamos que A y B son semigrupos.

1) Si $x, y, z \in A$ entonces

$$f(x * y * z) = f(x) * f(y) * f(z)$$

o, en general, si $x_1, .. x_n$ denotan elementos de A se tiene

$$f(x_1 * .. * x_n) = f(x_1) * .. * f(x_n)$$

en particular si $x_1 = .. = x_n = x$

$$f(x^n) = f(x)^n$$

2) Si A y B poseen ambos elementos identidad, que denotamos por e, y si $x \in A$ posee un inverso a la izquierda y' se tiene

$$f(y) * f(x) = f(y * x) = f(e) = e$$

por lo tanto f(y) es un inverso a la izquierda de f(x). Nótese el uso de la hipótesis f(e) = e. Análogamente, se tiene el resultado para un inverso a la derecha. Reuniendo los dos resultados se tiene que si x posee un inverso x' en A entonces f(x) posee un inverso f(x') en B y por la unicidad del inverso se tiene

$$\boxed{f(x') = f(x)'}$$

Por lo tanto

$$f : A \to B$$

restringida al subsemigrupo U(A) induce un morfismo que se denota también por f:

$$f : U(A) \to U(B)$$

Nota. Para los semigrupos numéricos donde la ley de composición es la suma, la relación $f(x') = f(x)'$ se interpreta como $f(-x) = -f(x)$. Para el caso multiplicativo la interpretación es $f(x^{-1}) = f(x)^{-1}$.

Ejercicio. Sea A un semigrupo y sea B un monoide. Probar que si existe un morfismo sobre $f: A \to B$, B es un semigrupo. Además, si $e \in A$ es elemento identidad entonces f(e) es elemento identidad de B.

Ejemplos

0. Sea (A, *) un monoide. La aplicación $id_A : A \to A$ es un morfismo que llamamos el morfismo identidad de A.

1. Sean (A, *, e) y (B, *, e) monoides con identidad. Entonces la aplicación constante f: $A \to B$ definida por

$$f(x) = e$$

cualquiera que sea $x \in A$ es un morfismo, que llamamos el morfismo trivial (de A en B).

2. Sean los monoides ($\mathbf{Q}$, +, 0) y ($\mathbf{Z}$, +, 0). Demostremos que el único morfismo de $\mathbf{Q}$ en $\mathbf{Z}$ es el dado por el ejemplo anterior, o sea que

$$f(q) = 0 \text{ cualquiera que sea } q \in \mathbf{Q}$$

Sea, en efecto, $f : \mathbf{Q} \to \mathbf{Z}$ un morfismo y sea $r/s \in \mathbf{Q}$.

Entonces

$$\begin{aligned} f(r/s) &= f(2r/2s) = f(2(r/2s)) = f(r/2s + r/2s) \\ &= f(r/2s) + f(r/2s) \\ &= 2 \cdot f(r/2s) \end{aligned}$$

y en general, si $n \in \mathbf{N}$,

$$\begin{aligned} f(r/s) &= f(nr/ns) = f(n(r/ns)) = f(\underbrace{r/ns + \ldots + r/ns}_{n \text{ veces}}) \\ &= f(r/ns) + \ldots + f(r/ns) \\ &= n \cdot f(r/ns) \end{aligned}$$

Se sigue entonces que el número entero (!)

$$f(r/s)$$

es divisible en $\mathbf{Z}$ por cualquier entero positivo n. Esto es posible sólo si

$$f(r/s) = 0$$

dado que cualquier número entero no nulo posee sólo un número finito de factores (consecuencia del Teorema Fundamental de la Aritmética). Siendo $r/s \in \mathbf{Q}$ arbitrario, nuestra afirmación queda probada. (Este ejemplo ilustra también la discusión informal que se presenta al comienzo de esta sección. En efecto, en el monoide $\mathbf{Q}$ es válida la divisibilidad por enteros no nulos, es decir, que cualquiera que sea $x \in \mathbf{Q}$ y cualquiera que sea $n \in \mathbf{N}$ existe $y \in \mathbf{Q}$ tal que

$$x = n \cdot y$$

Ahora puesto que

$$x = n \cdot y = y + y + \ldots + y \quad (n \text{ veces})$$

y f es un morfismo

$$f(x) = n \cdot f(y)$$

de manera que "f preserva la divisibilidad por enteros no nulos". Puesto que este tipo de divisibilidad --o sea para todo n-- no es válido en $\mathbf{Z}$, salvo para el caso trivial

$$0 = n \cdot 0$$

se entiende bien que el único morfismo de $\mathbf{Q}$ en $\mathbf{Z}$ debe ser el trivial).

3. Sea $(A, *)$ un semigrupo conmutativo. Para cada $n \in \mathbf{N}$ la aplicación

$$f_n : A \to A$$

definida por

$$x \to x^n$$

es un morfismo del monoide A en sí mismo. En efecto, esto es consecuencia de las relaciones

$$(x * y)^n = x^n * y^n$$

válidas en un semigrupo conmutativo. Ilustremos especializando A.

i. $(A, *) = (\mathbf{N}, .)$

$$f_n(x) = x \cdot x \ldots x = x^n$$

ii. $(A, *) = (\mathbf{N}, +)$

$$f_n(x) = x + x + \ldots + x = nx$$

iii. Sea $(A, *)$ el semigrupo definido por la tabla siguiente:

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	6	4	5
3	3	1	2	5	6	4
4	4	5	6	1	2	3
5	5	6	4	3	1	2
6	6	4	5	2	3	1

Notemos que este semigrupo no es conmutativo. Veremos que f_2 no es un morfismo de A en A.

En efecto, puesto que

$$4 * 5 = 2$$

debería tenerse

$$f_2(4 * 5) = f_2(4) * f(5) = 4^2 * 5^2 = 1 * 1 = 1$$

y además

$$f_2(4 * 5) = f_2(2) = 2^2 = 3$$

Por lo tanto f no es un morfismo a causa de la no conmutatividad de $*$.

G. Submonoides Asociados a Un Morfismo

Sean $(A, *, e)$ y $(B, *, e)$ monoides con identidad y sea

$$f : A \rightarrow B$$

un morfismo.

Sean los subconjuntos

$$\mathrm{Im}(f) \subset B$$
$$\mathrm{Nu}(f) \subset A$$

definidos por

$$\mathrm{Im}(f) = \{y \;/\; y \in B \text{ y existe } x \in A \text{ con } f(x) = y\}$$
$$\mathrm{Nu}(f) = \{x \;/\; f(x) = e\}$$

Proposición

a) $\mathrm{Im}(f)$ es submonoide de B.

b) $\mathrm{Nu}(f)$ es submonoide de A.

Demostración

a) Sean $y_1, y_2 \in \mathrm{Im}(f)$. Por su definición existen $x_1, x_2 \in A$ tales que

$$f(x_1) = y_1$$
$$f(x_2) = y_2$$

y siendo f un morfismo

$$y_1 * y_2 = f(x_1) * f(x_2) = f(x_1 * x_2)$$

lo cual demuestra que

$$y_1 * y_2 \in \mathrm{Im}(f)$$

Notemos que $f(e) = e$ implica $\mathrm{Im}(f) \neq \emptyset$.

b) Sean $x_1, x_2 \in \mathrm{Nu}(f)$. Por su definición se verifica

$$f(x_1) = e$$
$$f(x_2) = e$$

y siendo f un morfismo

$$e = e * e = f(x_1) * f(x_2) = f(x_1 * x_2)$$

lo cual demuestra que

$$x_1 * x_2 \in \mathrm{Nu}(f)$$

Notemos que $f(e) = e$ implica que $\mathrm{Nu}(f) \neq \emptyset$.

Definición. Los submonoides de la proposición anterior se denominan submonoides asociados a f; en particular se denominan

Im (f) imagen de f
Nu (f) núcleo de f

Ejemplos

1. Sean $(A, *, e)$ y $(B, *, e)$ monoides. Si f denota el morfismo trivial $f(x) = e$, se tiene

$$\mathrm{Im}(f) = \{e\}$$
$$\mathrm{Nu}(f) = A$$

2. Sea (A, *, e) un monoide y sea f el morfismo identidad id_A, o sea f(x) = x. Se tiene

$$Im(f) = A$$
$$Nu(f) = \{e\}$$

3. Sea (A, *, e) = (Z, . , 1) y (B, *, e) = (**N** ∪ {0}, . , 1). Sea f : **Z** → **N** ∪ {0} el morfismo f = f_2 o sea

$$f(x) = x^2$$

Entonces

$$Im(f) = \{0, 1, 4, 9, 16, ..\} = \{n^2 / n \in N\} \cup \{0\}$$
$$Nu(f) = \{-1, 1\}$$

4. Sea (A, *, e) el monoide definido por la tabla

*	0	2	1	3
0	0	2	1	3
2	2	0	3	1
1	1	3	2	0
3	3	1	0	2

Sea (B, *, e) el monoide definido por la tabla

*	a	b
a	a	b
b	b	a

La aplicación f : A → B definida por

f(0) = a f(2) = a
f(1) = b f(3) = b

es un morfismo (según podrá verificar el lector). Se tiene

$$Im(f) = B$$
$$Nu(f) = \{0, 2\}$$

H. Semigrupo de Morfismos

Sean (A, *), (B, *) y (C, *) monoides. Sean

$$g : A \to B$$
$$\text{y} \quad f : B \to C$$

morfismos. Entonces la composición

$$f \circ g : A \to C$$

es un morfismo. En efecto, sean x, y ε A

$$\begin{aligned}(f \circ g)(x * y) &= f(g(x * y)) \\ &= f(g(x) * g(y)) \\ &= f(g(x) * f(g(y)) \\ &= (f \circ g)(x) * (f \circ g)(y)\end{aligned}$$

Además, si A, B y C son todos monoides con elemento identidad e, resulta

$$(f \circ g)(e) = f(g(e)) = f(e) = e$$

queda por tanto probado que f o g es un morfismo.

La discusión precedente nos lleva a definir un semigrupo de suma importancia. En efecto, aplicando lo anterior a la situación

$$A = B = C$$

se tiene que si f y g son morfismos de A en A:

$$f : A \to A \text{ y } g : A \to A$$

la composición

$$f \circ g : A \to A$$

es un morfismo de A.

Proposición. Si End (A) denota la totalidad de endomorfismos de A entonces

$$(f, g) \to f \circ g$$

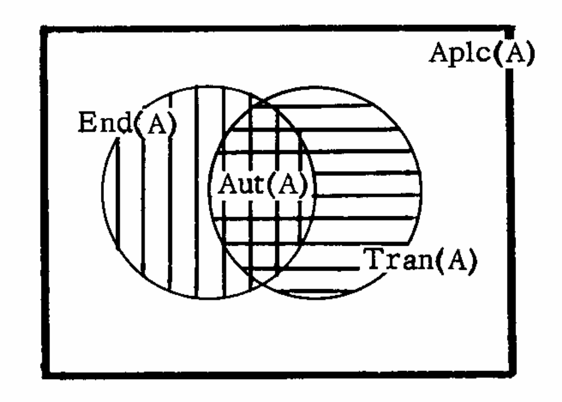
define sobre End (A) una estructura de monoide con identidad.

Además, (End (A), o) es un semigrupo y es subsemigrupo de Aplc(A).

Demostración. La proposición queda enteramente probada mostrando que End(A) es un submonoide del semigrupo Aplc(A) de "aplicaciones" de A en A. Lo dicho anteriormente prueba eso efectivamente. El elemento $e = id_A$ identidad de Aplc(A) es un morfismo y por lo tanto pertenece a End(A).

Definición. End(A) = (End(A), o) recibe el nombre de semigrupo de endomorfismos de (el monoide) A.

En el dibujo siguiente se muestra los distintos semigrupos asociados al monoide A. La "zona" designada por Aut(A) será objeto de estudio más adelante.



I. Tipos de Morfismos

Al lector puede resultarle ahora natural la idea de introducir morfismos que le permitan relacionar diferentes (o aparentemente diferentes) estructuras algebraicas (en este caso se trata de monoides). Hay además otra razón para introducir morfismos, y es ésta, en el fondo, la razón fundamental. En álgebra al estudiar un cierto tipo de estructura (monoide, grupo, anillo, etc.) se consideran dos tipos de modelos o ejemplos: abstractos y concretos. Así, un modelo abstracto de monoide consiste en un conjunto A y una ley de composición * de manera que los elementos del conjunto son entes abstractos sobre los cuales no damos ninguna descripción, y lo mismo sucede con respecto a la ley de composición. Un modelo concreto de monoide es aquél en que los elementos de A admiten una representación matemática; por ejemplo, son números, rotaciones, transformaciones, aplicaciones de un conjunto en otro, y la ley de composición admite una representación natural en términos de dichos objetos. De tal forma, si los elementos de A son transformaciones, entonces la ley de composición puede ser la composición de transformaciones.

Resulta en tal caso importante para el estudio de las estructuras algebraicas poseer un modo de "representar estructuras abstractas mediante estructuras concretas". En nuestra situación de monoides, por ejemplo, interesa poder representar monoides abstractos en monoides concretos. Así, si A es un monoide abstracto interesa encontrar un monoide concreto M (un monoide numérico o un monoide de aplicaciones) y un morfismo $f : A \rightarrow M$ que conserve al máximo la estructura de A. Esta idea lleva naturalmente a la definición siguiente.

Definición. Un morfismo $f : A \rightarrow B$ de monoides se designará un monomorfismo si la aplicación f es inyectiva, o sea si

cualesquiera que sean $x, y \in A$, $x \neq y \Rightarrow f(x) \neq f(y)$

Un monomorfismo $f : A \to B$ permite "identificar" A a un submonoide de B. En efecto, Im(f) es un submonoide de B y la identificación es

$$a \to f(a)$$

Ejemplo. Sean los monoides dados por las tablas de composición:

A

*	a	b
a	a	b
b	b	a

B

*	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

La aplicación

$$f : A \to B$$

definida por

$$f(a) = 0$$
$$f(b) = 2$$

define un monomorfismo de A en B y "vía" f es entonces posible identificar A con el submonoide $\{0, 2\}$ de B.

Sea ahora $f : A \to B$ un monomorfismo de monoides tal que

$$\text{Im}(f) = B$$

entonces A es identificable a B y así los monoides A y B son algebraicamente indistinguibles. Este es el concepto importante de isomorfismo

Definición. Sea $f : A \to B$ un morfismo de monoides. Diremos que f es un <u>isomorfismo</u> si

i. f es un monomorfismo
ii. $\text{Im}(f) = B$

En otros términos, f es un isomorfismo si f como aplicación de A en B es biyectiva.

Un criterio útil para determinar si un morfismo es un isomorfismo es el siguiente:

Teorema. Un morfismo $f : A \to B$ de monoides es un isomorfismo si, y sólo si, existe un morfismo $g : B \to A$ tal que las composiciones

$$g \circ f \quad \text{y} \quad f \circ g$$

satisfacen

$$g \circ f = id_A \quad y \quad f \circ g = id_B$$

Demostración. Sea, primeramente, $g: B \to A$ un morfismo que satisface las condiciones del teorema tal que

$$g \circ f = id_A \quad y \quad f \circ g = id_B$$

vamos a probar que f es un isomorfismo, es decir que f es biyectiva. Esto se debe al hecho de ser g una aplicación inversa de f. Para conveniencia del lector repetimos la demostración:

f es inyectiva : sean $x, y \in A$ entonces
$f(x) = f(y)$ implica $g(f(x) = g(f(y)$, o sea
$(g \circ f)(x) = (g \circ f)(y)$, o sea $x = y$

f es sobre : sea $z \in B$, entonces $g(z) \in A$ satisface
$z = id_B(z) = (f \circ g)(z) = f(g(z))$

Recíprocamente, sea f un isomorfismo. f es entonces una aplicación biyectiva de A en B y por lo tanto existe una "aplicación" inversa $g: B \to A$, es decir una aplicación que satisface

$$g \circ f = id_A \quad y \quad f \circ g = id_B$$

Se trata ahora solamente de probar que g es un morfismo. Sean pues $z, v \in B$. Entonces

$$f(g(v)) = v \quad y \quad f(g(z)) = z$$

de manera que

$$\begin{aligned} z * v &= f(g(z)) * f(g(v)) \quad \text{(y siendo f morfismo)} \\ &= f(g(z) * g(v)) \end{aligned}$$

Por lo tanto (aplicando g y utilizando $g \circ f = id_A$)

$$\begin{aligned} g(z * v) &= g(f(g(z) * g(v))) \\ &= (g \circ f)(g(z) * g(v)) \\ &= id_A(g(z) * g(v) \\ &= g(z) * g(v) \end{aligned}$$

lo cual demuestra que g es un morfismo.

Corolario. Con la notación del teorema anterior, g es un isomorfismo de B en A.

Demostración. Es consecuencia del papel simétrico que juegan f y g en la condición del teorema.

Definición. Diremos que un monoide A es isomorfo a un monoide B si existe un isomorfismo $f: A \to B$.

Del teorema anterior (y su corolario) se desprende:

Teorema. Sean A, B y C monoides

i. Si A es isomorfo a B entonces B es isomorfo a A.
ii. Si A es isomorfo a B y B es isomorfo a C, entonces A es isomorfo a C.

Demostración.

i. es consecuencia del corolario.
ii. Sean $f : A \to B$ y $g : B \to C$ isomorfismos. Existe entonces morfismos $f' : B \to A$ y $g' : C \to B$ tales que

$$f' \circ f = id_A, \quad f \circ f' = id_B$$
$$g' \circ g = id_B, \quad g \circ g' = id_C$$

Por lo tanto

$$\begin{aligned}(g \circ f) \circ (f' \circ g') &= g \circ (f \circ f') \circ g' = g \circ id_B \circ g' \\ &= g \circ g' \\ &= id_C \\ (f' \circ g') \circ (g \circ f) &= f' \circ (g' \circ g) \circ f = f' \circ id_B \circ f \\ &= f' \circ f \\ &= id_A\end{aligned}$$

Por lo tanto

$$f' \circ g' : C \to A$$

es morfismo inverso de

$$g \circ f : A \to C$$

y, en virtud del teorema anterior, $g \circ f$ es un isomorfismo de A en C, o sea A es isomorfo a C.

Aplicación. Analicemos el caso de isomorfismos de A en sí mismo. Sean Aplc (A), Tran(A) y End (A) los semigrupos de aplicaciones de A, de transformaciones de A y de endomorfismos de A, respectivamente. Sabemos que Tran(A) y End (A) son subsemigrupos de Aplc (A).

Definición. Llamaremos <u>automorfismo de A</u> a todo isomorfismo de A en sí mismo. Con Aut (A) denotamos la totalidad de automorfismos de A. Se tiene entonces los siguientes resultados:

1) $\boxed{Aut(A) = Tran(A) \cap End(A)}$

2) $\boxed{Aut(A) = U(End(A))}$

Por lo tanto Aut (A) es un semigrupo, que denominamos el semigrupo de automorfismos del monoide A.

Señalemos un tipo particular de automorfismos de un semigrupo $(A, *, e)$ determinados intrínsecamente por A. Sea $u \in A$ un elemento inversible. Consideremos la aplicación $g: A \to A$ definida por

$$g(a) = u * a * u'$$

Afirmamos que g es un automorfismo de A. En efecto,

$$\begin{aligned} g(a_1 * a_2) &= u * (a_1 * a_2) * u' \\ &= u * a_1 * (u' * u) * a_2 * u' \\ &= (u * a_1 * u') * (u * a_2 * u') \\ &= g(a_1) * g(a_2) \end{aligned}$$

Por lo tanto, g así definido es un endomorfismo. Probemos que g es un automorfismo. Será suficiente encontrar un inverso de g. Sea $h : A \rightarrow A$ definido por $h(a) = u' * a * u$. Entonces, por la misma demostración hecha para g, se tiene que h es un endomorfismo de A.

Puesto que además

$$\begin{aligned} (g \circ h)(a) &= g(u' * a * u) \\ &= u * (u' * a * u) * u' \\ &= a \\ (h \circ g)(a) &= h(u * a * u') \\ &= u' * (u * a * u') * u \\ &= a \end{aligned}$$

se tiene que h es inverso de g. O sea, $g \in Aut(A)$ conforme queríamos probar. Por lo tanto, si Int(A) es el conjunto de las aplicaciones así definidas,

$$Int(A) \subset Aut(A)$$

Notemos también que

$$id_A \in Int(A)$$

dado que

$$a = id_A(a) = e * a * e = e * a * e'$$

Sean $g, f \in Int(A)$ definidos por $u, v \in A$ mediante

$$\begin{aligned} g(a) &= u * a * u' \\ f(a) &= v * a * v' \end{aligned}$$

Entonces

$$\begin{aligned} (g \circ f)(a) &= g(v * a * v') = u * (v * a * v') * u' \\ &= (u * v) * a * (v' * u') \\ &= (u * v) * a * (u * v)' \end{aligned}$$

por lo tanto

$$g \circ f \in Int(A)$$

Se ha probado pues que Int(A) es submonoide de Aut(A). Los elementos de Int(A), denominados los <u>automorfismos</u> <u>interiores</u> de A, están por lo tanto determinados por los elementos inversibles de A. Notemos que si $u \in A$ es un elemento inversible tal que

$$u * a = a * u$$

entonces el automorfismo asociado a u es la identidad:

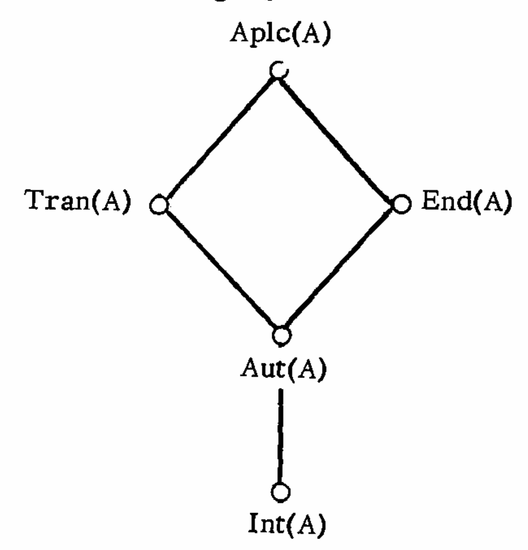
$$g(a) = u * a * u' = a * u * u' = a$$

En particular, si A es un semigrupo conmutativo

$$\mathrm{Int}(A) = \{id_A\}$$

Los elementos de Aut (A) que no están en Int (A) se suelen denominar automorfismos exteriores de A. Es siempre de interés conocer la existencia de automorfismos exteriores de un semigrupo dado.

El diagrama siguiente reúne los diferentes semigrupos asociados a un semigrupo (A, *, e). Los mismos están ordenados según la relación de "ser subsemigrupo de".



Ejemplos

1. Sea el monoide (A, *) definido por la siguiente tabla de composición:

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Vamos a determinar End (A) y Aut (A). Notemos primeramente que cualquiera que sea el endomorfismo f de A

$$\boxed{f(0) = 0 \quad \text{ó} \quad f(0) = 1}$$

En efecto, si $x \in A$ entonces $0 * x = 0$ implica

$$f(0) = f(0) * f(x)$$

Por lo tanto, si $f(0) \neq 0$ existe (según la tabla) $y \in A$ tal que

$$y * f(0) = 1$$

por lo tanto

$$1 = y * f(0) = y * f(0) * f(x) = f(x)$$

y siendo x arbitrario, f es el morfismo trivial. En particular $f(0) = 1$.

Tratándose además de un monoide con identidad 1 se verifica (dada la definición de morfismo) que

$$\boxed{f(1) = 1}$$

cualquiera que sea $f \in \text{End}(A)$.

Además, si $x \in A, x \neq 0$ entonces

$$f(x) = 0$$

es imposible. En efecto, $x \neq 0$ implica (según la tabla) la existencia de $x' \in A$ tal que $x' * x = 1$, por lo tanto

$$\begin{aligned} f(x) = 0 \text{ implica } 1 &= f(1) = f(x' * x) = \\ &= f(x') * f(x) \\ &= f(x') * 0 \\ &= 0 \end{aligned}$$

lo cual es un absurdo.

Nótese asimismo que

$$\begin{aligned} 2 * 2 &= 4 \\ 2 * 2 * 2 &= 3 \\ 2 * 2 * 2 * 2 &= 1 \end{aligned}$$

implica para un morfismo f, que los valores

$$f(4), \quad f(3)$$

están condicionados al valor $f(2)$.

Investiguemos, por lo tanto, los valores posibles de $f(2)$. Resulta

a) Si $f(2) = 1$ entonces $f(1) = f(3) = f(4) = 1$

b) Si $f(2) = 2$ entonces $f(1) = f(2^4) = f(2)^4 = 1$
$f(3) = f(2^3) = f(2)^3 = 3$
$f(4) = f(2^2) = f(2)^2 = 4$

c) Si $f(2) = 3$ entonces $f(1) = f(2)^4 = 3^4 = 1$
$f(3) = f(2)^3 = 3^3 = 2$
$f(4) = f(2)^2 = 3^2 = 4$

d) Si $f(2) = 4$ entonces $f(1) = f(2)^4 = 4^4 = 1$
$f(3) = f(2)^3 = 4^3 = 4$
$f(4) = f(2)^2 = 4^2 = 1$

Recíprocamente, si definimos aplicaciones $f: A \to A$ según a), b), c) y d) obtenemos, como es fácil verificar, endomorfismos de A. Se tiene en definitiva que End (A) consta de los 5 endomorfismos, que se describen a continuación.

x	$f_0(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	1	0	0	0	0
1	1	1	1	1	1
2	1	2	1	3	4
3	1	3	1	2	4
4	1	4	1	4	1

Se sigue que

$$\text{Aut}(A) = \{f_1, f_3\}$$

La tabla de composición de End (A) es la siguiente:

o	f_0	f_1	f_2	f_3	f_4
f_0	f_0	f_0	f_0	f_0	f_0
f_1	f_0	f_1	f_2	f_3	f_4
f_2	f_0	f_2	f_2	f_2	f_2
f_3	f_0	f_3	f_2	f_1	f_4
f_4	f_0	f_4	f_2	f_4	f_2

2. Sea $A = (\mathbf{N}, +)$ el monoide aditivo de los números naturales. Si f es un endomorfismo de A y si

$$f(1) = a$$

entonces

$$f(2) = f(1+1) = f(1) + f(1) = a + a$$
$$= 2 \cdot a$$
$$\dots$$
$$f(n) = n \cdot a$$

es decir, f está unívocamente determinada por el valor que toma sobre 1, o sea por $a = f(1)$. Recíprocamente, si $a \in \mathbf{N}$ podemos definir la aplicación

$$g: N \to N$$
$$g(n) = n \cdot a$$

la cual satisface

$$f(n+m) = (n+m) \cdot a = n \cdot a + m \cdot a$$
$$= f(n) + f(m)$$

o sea que g es un morfismo de A.

La discusión precedente permite afirmar que los morfismos de $A = (\mathbf{N}, +)$ están unívocamente determinados por los elementos de $\mathbf{N}$, por lo tanto si $f \in End(A)$ escribiremos

$$f = \mathcal{g}_a \quad si \quad f(1) = a$$

En estas condiciones queda definida una aplicación

$$\mathcal{g} : \mathbf{N} \to End(A)$$

por

(*) $$\mathcal{g} : a \to \mathcal{g}_a$$

Veamos qué propiedades posee $\mathcal{g}$. Sean $a, b \in \mathbf{N}$, está definido entonces el endomorfismo $\mathcal{g}_{a.b}$ de A:

$$\mathcal{g}_{a.b}(m) = m \cdot (a \cdot b)$$

El mismo satisface

$$\begin{aligned} \mathcal{g}_{a.b}(m) &= m \cdot (a \cdot b) = (m \cdot a) \cdot b \\ &= \mathcal{g}_b(m \cdot a) \\ &= \mathcal{g}_b(\mathcal{g}_a(m)) \\ &= (\mathcal{g}_b \circ \mathcal{g}_a)(m) \end{aligned}$$

o sea

$$\mathcal{g}_{a.b} = \mathcal{g}_b \circ \mathcal{g}_a$$

y puesto que

$$a \cdot b = b \cdot a \Rightarrow \mathcal{g}_{a.b} = \mathcal{g}_{b.a}$$

se tiene

(**) $$\boxed{\mathcal{g}_{a.b} = \mathcal{g}_a \circ \mathcal{g}_b}$$

Además, puesto que

$$\mathcal{g}_a = \mathcal{g}(a) \qquad (\text{según } (*))$$

(**) se escribe también

$$\boxed{\mathcal{g}(a \cdot b) = \mathcal{g}(a) \circ \mathcal{g}(b)}$$

o sea "la aplicación

$$\mathcal{g} : \mathbf{N} \to End(A)$$

es un morfismo del monoide $(\mathbf{N}, .)$ en el monoide $(End(A), \circ)$". Asimismo dado que todo endomorfismo de A es de la forma $\mathcal{g}_a (= \mathcal{g}(a))$ y $\mathcal{g}_a = \mathcal{g}_b$ implica $a = b$, se tiene que

$$\mathcal{g} : (\mathbf{N}, .) \to End(A)$$

es un isomorfismo.

Nótese finalmente que el único elemento inversible de $(N, .)$ es el elemento unidad 1, o sea $U((\mathbf{N}, .)) = \{1\}$. Por tanto, el único elemento inversible de End (A) debe ser $\mathcal{g}_1$ que no es otra cosa que

$$\mathcal{g}_1 = id_A$$

por lo tanto

$$Aut(A) = \{id_A\}$$

A manera de ejercicio, se deja al lector desarrollar un ejemplo análogo al anterior en la situación siguiente (A, *) = ($\mathbf{Z}$, +) el monoide aditivo de los números enteros. El resultado será

$$\mathrm{End}(A) \simeq (\mathbf{Z}, .)$$
$$\mathrm{Aut}(A) \simeq \{1, -1\}$$

3. Sea A = {1, 2, 3, 5, 6, 10, 15, 30} = totalidad de divisores de 30. Entonces $a_1 * a_2 = (a_1, a_2)$ = máximo común divisor de a_1 y a_2 define sobre A una estructura de semigrupo con identidad e = 30. Sea X = {2, 3, 5} = totalidad de divisores primos de 30. Sea C = $\mathcal{P}$(X) = la totalidad de partes de X. Sea (C, ∩) el monoide definido por la intersección ∩ de conjuntos. C es entonces un semigrupo con identidad e = X. A y C admiten la siguiente descripción:

A:

(,)	1	2	3	5	6	10	15	30
1	1	1	1	1	1	1	1	1
2	1	2	1	1	2	2	1	2
3	1	1	3	1	3	1	3	3
5	1	1	1	5	1	5	5	5
6	1	2	3	1	6	2	3	6
10	1	2	1	5	2	10	5	10
15	1	1	3	5	3	5	15	15
30	1	2	3	5	6	10	15	30

C:

∩	∅	{2}	{3}	{5}	{2, 3}	{2, 5}	{3, 5}	X
∅	∅	∅	∅	∅	∅	∅	∅	∅
{2}	∅	{2}	∅	∅	{2}	{2}	∅	{2}
{3}	∅	∅	{3}	∅	{3}	∅	{3}	{3}
{5}	∅	∅	∅	{5}	∅	{5}	{5}	{5}
{2, 3}	∅	{2}	{3}	∅	{2, 3}	{2}	{3}	{2, 3}
{2, 5}	∅	{2}	∅	{5}	{2}	{2, 5}	{5}	{2, 5}
{3, 5}	∅	∅	{3}	{5}	{3}	{5}	{3, 5}	{3, 5}
X	∅	{2}	{3}	{5}	{2, 3}	{2, 5}	{3, 5}	X

Sea ahora

$$f : C \to A$$

definida por

$$f(\emptyset) = 1 \quad f(\{2\}) = 2 \quad f(\{3\}) = 3 \quad f(\{5\}) = 5$$
$$f(\{2,3\}) = 6 \quad f(\{2,5\}) = 10 \quad f(\{3,5\}) = 15$$
$$f(X) = 30$$

f es evidentemente una aplicación biyectiva de C en A. Además, observando ambas tablas de composición vemos que f es un morfismo. En definitiva, f es un isomorfismo.

Nota. El ejemplo anterior es un caso particular de la siguiente situación general, cuya demostración no es difícil y puede ser un ejercicio útil para el lector. Sea s un entero positivo con la propiedad siguiente:

ningún divisor de s, excepto 1, es un cuadrado

(por ejemplo: s = 15, 21, 210, . .). Entonces, si A designa el monoide de la totalidad de divisores de s con la ley de composición máximo común divisor, y si C es el monoide de la totalidad de partes del conjunto de divisores primos de s con la ley de composición intersección, se tiene que A y C son monoides isomorfos. El isomorfismo puede establecerse mediante la aplicación $f : C \to A$ que asocia a cada subconjunto no vacío de factores primos de s el producto de los mismos, y que asocia 1 al conjunto vacío, en símbolos

$$\emptyset \to 1$$
$$\{p_1, \ldots, p_k\} \to p_1 \cdots p_k$$

(¡ El lector puede investigar qué sucede si s es divisible por un cuadrado $\neq 1$!)

4. Sea X un conjunto y sea $\mathcal{P}(X)$ el conjunto de partes de X. Sean sobre $\mathcal{P}(X)$ las dos siguientes estructuras de monoides

$$A = (\mathcal{P}(X), \cup)$$
$$B = (\mathcal{P}(X), \cap)$$

Sea $f : A \to B$ la aplicación

$$f(V) = \complement V = X - V \text{ (= complemento de V en X)}$$

es fácil ver que f es una aplicación biyectiva.

Ahora, en virtud de una de las leyes de De Morgan se tiene

$$f(V_1 \cup V_2) = \complement(V_1 \cup V_2) = (\complement V_1) \cap (\complement V_2)$$
$$= f(V_1) \cap f(V_2)$$

por lo tanto, f establece un isomorfismo de ambas estructuras.

J. Construcción de Nuevos Monoides

En esta sección vamos a estudiar la construcción de monoides a partir de monoides dados.

a. Monoide de aplicaciones

Sea (A, *) un monoide. Sea X un conjunto no vacío. Consideremos el conjunto denotado por

$$\mathrm{Apl}(X, A)$$

formado por todas las aplicaciones X en A. Vamos a definir en Apl (X, A) una ley de composición. La definición es completamente natural: sean f, g ϵ Apl (X, A) y sea x ϵ X, entonces

$$f(x) \in A \quad y \quad g(x) \in A$$

por lo tanto

$$f(x) * g(x) \in A$$

Definición. La aplicación de X en A definida por

$$x \rightarrow f(x) * g(x)$$

la denotaremos por

$$f * g$$

y la denominaremos la composición puntual de f con g. Es claro que la composición puntual define en Apl (X, A) una estructura de monoide que denominaremos el monoide de aplicaciones de X en A.

Proposición. Sea (Apl (X, A), *) el monoide de aplicaciones de X en A.

i. Si A es semigrupo entonces Apl (X, A) es semigrupo.
ii. Si A es conmutativo entonces Apl (X, A) es conmutativo.
iii. Si A posee identidad (respectivamente, a la derecha y a la izquierda) entonces Apl (X, A) posee identidad (respectivamente a la derecha y a la izquierda).

Demostración

i. Debemos probar la sociatividad f * (g * h) = (f * g) * h, si f, g, h ϵ Apl (X, A). Recordamos al lector que dicha igualdad equivale a probar que cualquiera que sea x ϵ X:

$$(f * (g * h))(x) = ((f * g) * h)(x)$$

Entonces

$$\begin{aligned}(f * (g * h))(x) &= f(x) * ((g * h)(x)) \\ &= f(x) * ((g(x) * h(x)) \\ &= (f(x) * g(x)) * h(x) \\ &= ((f * g)(x)) * h(x) \\ &= ((f * g) * h)(x)\end{aligned}$$

conforme se deseaba probar.

ii. Su demostración queda como ejercicio para el lector.
iii. Sea $e \in A$ identidad a la izquierda. Sea $\underline{e} : X \to A$ la aplicación de X en A definida por

$$\underline{e}(x) = e$$

cualquiera que sea $x \in X$.

Entonces $\underline{e}$ satisface:

$$\begin{aligned}(\underline{e} * f)(x) &= \underline{e}(x) * f(x)\\ &= e * f(x)\\ &= f(x)\end{aligned}$$

de manera que

$$\underline{e} * f = f$$

y $\underline{e}$ resulta una identidad a la izquierda.

b. Suma directa de monoides

Sean $(A_1, *)$ y $(A_2, *)$ monoides. Sea

$$A = A_1 \times A_2$$

el producto cartesiano de los conjuntos A_1 y A_2. Vamos a definir una ley de composición en A como sigue

$$(x_1, y_1) * (x_2, y_2) = (x_1 * x_2,\ y_1 * y_2)$$

$x, x_2 \in A_1$, $y_1, y_2 \in A_2$.

En esta forma, A se convierte en un monoide $(A, *)$ que denominamos la suma directa de $(A_1, *)$ y $(A_2, *)$. Se tiene además la proposición siguiente.

Proposición

i. Si $(A_1, *)$ y $(A_2, *)$ son semigrupos, entonces $(A, *)$ es semigrupo.
ii. Si $(A_1, *)$ y $(A_2, *)$ son ambos monoides conmutativos, entonces $(A, *)$ es conmutativo.
iii. Si $(A_1, *)$ posee identidad (respectivamente identidad a la izquierda) y $(A_2, *)$ posee identidad (respectivamente identidad a la izquierda), entonces $(A, *)$ posee identidad (respectivamente identidad a la izquierda).

Demostración. Queda como ejercicio para el lector.

En forma análoga se puede definir la suma directa de cualquier número $(A_1, *), \ldots, (A_n, *)$ de monoides.

Notación. La suma directa de monoides $(A_1, *), \ldots, (A_n, *)$ se denota por

$$A_1 \oplus A_2 \oplus \ldots \oplus A_n.$$

Ejemplo. Sean los monoides

A_1

*	0	1
0	0	1
1	1	0

A_2

*	a	b
a	a	a
b	a	b

entonces

$A_1 \oplus A_2$

*	(0, a)	(0, b)	(1, a)	(1, b)
(0, a)	(0, a)	(0, a)	(1, a)	(1, a)
(0, b)	(0, a)	(0, b)	(1, a)	(1, b)
(1, a)	(1, a)	(1, a)	(0, a)	(0, a)
(1, b)	(1, a)	(1, b)	(0, a)	(0, b)

II. ESTRUCTURA DE GRUPO

A. Definición y Ejemplos

En el capítulo anterior asociamos a todo semigrupo A con identidad el semigrupo U (A) de elementos inversibles de A. Las propiedades esenciales de U (A) son las siguientes:

g1)	U (A) es un semigrupo con elemento identidad.
g2)	Todo elemento de U (A) es inversible.

Estas dos propiedades dan lugar a la estructura de mayor importancia, no sólo en álgebra, sino en la matemática misma, a saber: la ESTRUCTURA DE GRUPO.

Definición. Se dice que un monoide (A, *) posee estructura de grupo, o simplemente que A es un grupo, si se satisfacen las dos condiciones siguientes:

g1) (A, *) es un semigrupo con identidad.
g2) Todo elemento de A es inversible.

Explícitamente las condiciones de definición de grupo se escriben así:

g1): * es una ley de composición asociativa, o sea tal que

$$x * (y * z) = (x * y) * z$$

cualesquiera que sean x, y, z en A.
Existe $e \in A$ tal que $x * e = e * x = x$, cualquiera que sea x en A.

g2): Para todo $x \in A$ existe $x' \in A$ que satisface

$$x * x' = x' * x = e$$

Lo que se acaba de expresar más arriba permite obtener una amplia variedad de ejemplos de estructura de grupo, o sea, repitiendo, para todo semigrupo A con identidad U (A) = el conjunto de todos los elementos inversibles de A es un grupo. Los ejemplos que se indican en la tabla siguiente son de ese tipo:

A	U (A)
$(\mathbf{Z}, +, 0)$	$\mathbf{Z}$
$(\mathbf{Z}, ., 1)$	$\{1, -1\}$
$(\mathbf{N}, ., 1)$	$\{1\}$
$(\mathbf{Q}, +, 0)$	$\mathbf{Q}$
$(\mathbf{Q}, ., 1)$	$\mathbf{Q}\# = \mathbf{Q} - \{0\}$
$(\mathbf{R}, +, 0)$	$\mathbf{R}$
$(\mathbf{R}, ., 1)$	$\mathbf{R}\# = \mathbf{R} - \{0\}$

(Cont.)

A	U (A)
$(\mathbf{C}, +, 0)$	$\mathbf{C}$
$(\mathbf{C}, \cdot, 1)$	$\mathbf{C}\# = \mathbf{C} - \{0\}$
Aplc (X)	Tran (X)
End (B)	Aut (B)

Ejemplo. Sea G la totalidad de números complejos z de la forma

$$z = a + i \cdot b \quad \text{donde } a, b \in \mathbf{Z}$$

(los elementos de G se denominan enteros de Gauss).

Sea * la ley de composición definida en G por el producto ordinario de números complejos:

Si $z = a + i \cdot b$ y $v = c + i \cdot d$ entonces

$$z * v = z \cdot v = (ac - bd) + i \cdot (ad + bc)$$

Es fácil ver que (G, *) es un semigrupo con identidad $e = 1 + i \cdot 0$ que denotamos 1. En efecto, G es subsemigrupo de $(\mathbf{C}, \cdot, 1)$.

Se trata ahora de encontrar el grupo U (G) de elementos inversibles de G. El siguiente es el procedimiento clásico.

Sea

$$N : G \to \mathbf{Z}$$

definido por

$$N : a + i \cdot b \to a^2 + b^2$$

Una verificación inmediata nos dice que

$$\boxed{N \text{ es un morfismo de } (G, *) \text{ en } (\mathbf{Z}, \cdot, 1)}$$

o sea

$$N(z * v) = N(z) \cdot N(v)$$

(Este morfismo recibe el nombre de norma.) Ahora, puesto que

$$x \in U(G) \Rightarrow N(x) \in U(\mathbf{Z}, \cdot, 1) = \{1, -1\}$$

se tiene que: $z = a + i \cdot b$ es inversible sólo si

$$N(z) = a^2 + b^2 \in \{1, -1\}$$

Pero $N(z) = -1$ es imposible por ser suma de cuadrados.

Entonces

$$\begin{aligned} N(z) &= a^2 + b^2 = 1, \text{ o sea} \\ z &= 1 + i \cdot 0 \text{ ó} \\ &= -1 + i \cdot 0 \text{ ó} \\ &= 0 + i \cdot 1 \text{ ó} \\ &= 0 + i \cdot -1 \end{aligned}$$

O sea: U (G) consta a lo sumo de 4 elementos.

Finalmente, dado que los elementos (*) son inversibles:

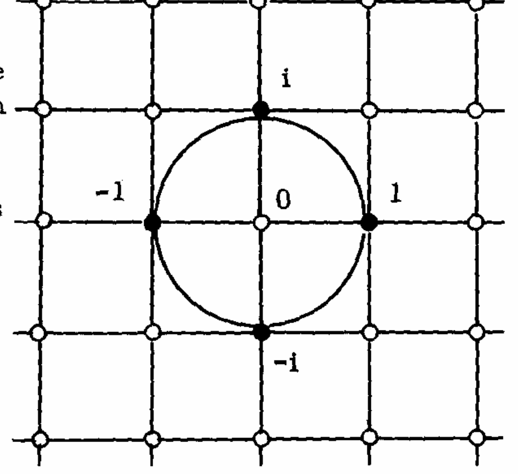
$$1 \cdot 1 = 1$$
$$(-1) \cdot (-1) = 1$$
$$i \cdot (-1) = 1$$
$$(-i) \cdot i = 1$$

se tiene:

$$\boxed{U(G) = \{1, -1, i, -i\}}$$

Dibujando los enteros de Gauss en el plano complejo se obtiene un reticulado y la intersección del mismo con la circunferencia unitaria (o sea de radio 1) nos da U (G):

Otros Ejemplos



1. Sea B un grupo y sea X un conjunto no vacío. Entonces el monoide Apl (X, B) de aplicaciones de X en B, con la composición puntual de aplicaciones, es un grupo y lo denominamos el grupo de aplicaciones de X en B.

2. Sean A_1 y A_2 grupos. Sea $A = A_1 \oplus A_2$ la suma directa de los monoides correspondientes. Entonces A posee estructura de grupo que denominamos igualmente la suma de A_1 y A_2.

Nota. La condición necesaria y suficiente para que un semigrupo con identidad A sea un grupo es que $A = U(A)$. Por lo tanto, se sigue que: todo grupo es realizable como grupo de elementos inversibles de un semigrupo. En esta forma, la construcción anterior permite obtener todos los ejemplos de estructura de grupo.

Ejercicio. Sea A un semigrupo finito. Si $z \in A$ denotamos con Az la totalidad de elementos de A de la forma $a * z$. Sean las siguientes condiciones definidas en A:

i. $a * x = a * y \Rightarrow x = y$

ii. $Ax \cap Ay \neq \emptyset$

Entonces: 1. Probar que si A satisface i e ii, entonces A es un grupo; 2. dar un ejemplo de semigrupo que satisface i, pero no es grupo, y 3. probar que si A es infinito, la afirmación en 1, no necesita ser válida.

B. Ecuaciones que Definen la Estructura de Grupo

Nuestro próximo paso es establecer las condiciones que permitan caracterizar la estructura de grupo dentro de la estructura

de semigrupo. En adelante al hablar de "ecuación sobre un monoide A" se entenderá cualquier expresión formal del tipo

$$a * X * b = c, \quad a * Y * b = c$$
$$a * X = c, \quad a * Y = c$$
$$X * b = c, \quad Y * b = c$$

donde a, b y c representan elementos de A y donde X, Y representan signos indeterminados (o simplemente indeterminadas). Cuando al reemplazar X, Y (o, como suele decirse, al especializar X, Y) por elementos x, y de A en alguna de las ecuaciones anteriores se obtiene una expresión verdadera, decimos que x, y son "soluciones" de las mismas. Esto es exactamente igual en los cursos elementales de álgebra o aritmética. Por ejemplo, si A posee elemento identidad e, entonces la ecuación

$$a * X = a$$

posee siempre una solución en A.

El teorema de caracterización de grupos está enunciado exactamente en términos de resolución de ecuaciones del tipo anterior. El lector está ya familiarizado con la idea, pero refresquémosla con un ejemplo. En el semigrupo (**N**, +), que no es un grupo, no todas las ecuaciones

$$n + X = m$$

poseen solución. Es más, las únicas que poseen solución son precisamente aquéllas en que $n < m$. En cambio, en el monoide (**Z**, +), que si es un grupo, las ecuaciones

$$n + X = m$$

poseen solución cualesquiera que sean n y m en **Z**. Justamente la definición de **Z** no es otra cosa que el conjunto obtenido a partir de **N** más las soluciones de las ecuaciones sobre **N**:

$$n + X = m$$

(Por ejemplo, 0 es la solución de $1 + X = 1$, -1 es la solución de la ecuación $2 + X = 1$, etc... .)

Teorema. Sea (A, *) un semigrupo. Entonces todas las proposiciones siguientes son equivalentes entre sí.

i. (A, *) es un grupo.

ii. Toda ecuación sobre A del tipo

(:) $$a * X * b = c$$

posee una <u>única</u> solución en A.

iii. Toda ecuación sobre A del tipo

$$a * X * b = c$$

posee una solución en A.

Demostración

i. $\Rightarrow$ ii. Sea una ecuación del tipo (:). Debemos encontrar una solución de la misma en A y demostrar además que esta solución es única. La manera de encontrar una solución es "despejando X". Sea

$$x = a' * c * b' \in A$$

Se tiene

$$\begin{aligned} a * x * b &= a * (a' * c * b') * b' \\ &= (a * a') * c * (b' * b) \\ &= e * c * e \\ &= c \end{aligned}$$

de manera que x es solución de (:). Probemos ahora que si $y \in A$ es también solución de (:) debe ser $x = y$. En efecto,

$$a * x * b = c = a * y * b$$

"Multiplicando" a la izquierda por a' y a la derecha por b' resulta

$$(a' * a) * x * (b * b') = (a' * a) * y * (b * b')$$

es decir

$$e * x * e = e * y * e$$

o sea finalmente

$$x = y$$

Queda pues probada la implicación i. $\Rightarrow$ ii.

ii. $\Rightarrow$ iii. Trivial.

iii. $\Rightarrow$ i. Sea $a \in A$. Por la hipótesis de resolubilidad de las ecuaciones del tipo (:) existe $x \in A$ que satisface

$$a * x * a = a$$

por lo tanto, llamando

$$e = a * x$$

se tiene

$$e * a = a$$
$$e^2 = e * e = e$$

Sea ahora $y \in A$ que satisface

$$a * y * e = a$$

entonces

$$\begin{aligned} a * e &= (a * y * e) * e = a * y * (e^2) \\ &= a * y * e \\ &= a \end{aligned}$$

Se ha demostrado pues que $e \in A$ satisface

(') $$a * e = e * a = a$$

(Notemos que e depende por ahora de a.) Sea $b \in A$. Existe $v \in A$ tal que

$$b = a * v * a$$

se sigue de (') que

$$\begin{aligned} e * b &= (e * a) * v * a = a * v * a \\ &= b \\ b * e &= a * v * (a * e) = a * v * a \\ &= b \end{aligned}$$

Se ha demostrado pues que el elemento e es identidad de $(A, *)$. Vamos a probar finalmente que todo $b \in A$ es inversible. Sean $z, w \in A$ tales que

$$\begin{aligned} e &= b * z * e = b * z \\ e &= e * w * b = w * b \end{aligned}$$

Es fácil ver entonces que $w = z$ es inverso de b.

Sigue por lo tanto la implicación iii $\Rightarrow$ i. El teorema queda completamente probado.

Se deja al lector el demostrar en forma análoga el siguiente teorema.

Teorema. Sea $(A, *)$ un semigrupo. Entonces las siguientes proposiciones son equivalentes entre sí.

j. $(A, *)$ es un grupo.

jj. Las ecuaciones sobre A, de los tipos

$$(::) \qquad \begin{aligned} a * X &= b \\ Y * c &= d \end{aligned}$$

poseen soluciones <u>únicas</u> en A.

jjj. Las ecuaciones sobre A (::) poseen soluciones en A.

Consideremos ahora algunas consecuencias del teorema anterior. Varios de los resultados que se dan a continuación fueron obtenidos anteriormente para semigrupos.

Sea A un grupo, $x, y \in A$

1) $x^2 = x$ implica $x = e =$ identidad de A. En efecto, x y e son ambas soluciones de

$$x * X = x$$

por lo tanto por jj debe ser $x = e$.

2) $(x')' = x$. En efecto, x y $(x')'$ son ambas soluciones de

$$x' * X = e$$

por lo tanto por jj debe ser $(x')' = x$.

3) $x * y = e$ implica $y = x'$. En efecto, x' e y son ambas soluciones de

$$x * X = e$$

4) $y * x = e$ implica $y = x'$. En efecto, por 3) $x = y'$ y por lo tanto $x' = (y')' = y$ según 2).

5) $e' = e$. En efecto, aplicando 3) (ó 4)) a la situación $e * e = e$ resulta $e = e'$.

Aquí el lector podría preguntarse si no sería suficiente, en el teorema precedente, la resolución de un solo tipo de las ecuaciones (::) para caracterizar la estructura de grupo. Es fácil comprobar que no. Sea en efecto, $(A, *)$ el monoide $(\mathbf{N}, *)$ donde $x * y = y$. Entonces todas las ecuaciones sobre A del tipo

$$a * X = b$$

poseen "única" solución en A. Sin embargo $(\mathbf{N}, *)$ no es un grupo. Notemos, por ejemplo, que si $c \neq d$, la ecuación

$$Y * c = d$$

no posee ninguna solución en A.

Finalmente, digamos que toda terminología utilizada en el tratamiento de monoides se aplica en particular a los grupos. Por ejemplo, un grupo conmutativo será un grupo cuya estructura de semigrupo es conmutativa. Análogamente, un morfismo de grupos $f : A_1 \to A_2$ significa un morfismo de los monoides correspondientes. Conviene observar que tratándose de grupos la condición

$$f(e) = e$$

es consecuencia de la condición

$$f(x * y) = f(x) * f(y)$$

En efecto, $f(e) \in A_2$ satisface

$$f(e) = f(e)^2$$

y ya vimos que el único elemento idempotente de un grupo es el elemento identidad. Citemos por último un resultado de suma utilidad.

Proposición. Sea A un grupo y sea B un semigrupo con elemento identidad. Sea $f : A \to B$ un morfismo. Entonces f es un monomorfismo si, y sólo si, $Nu(f) = \{e\}$.

Demostración. Sea f un monomorfismo. Si $x \in Nu(f)$ se tiene

$$f(x) = e = f(e)$$

por lo tanto $x = e$. Esto demuestra que $Nu(f) = \{e\}$.

Recíprocamente, sea $Nu(f) = \{e\}$. Si $x, z \in A$ son tales que

(o) $$f(x) = f(z)$$

entonces, siendo A un grupo existe $x' \in A$. Luego de (o)

$$f(x) * f(x') = f(z) * f(x')$$

o sea

$$e = f(e) = f(x * x') = f(z * x')$$

de manera que

$$z * x' \in Nu(f) = \{e\}$$

es decir

$$z * x' = e$$
$$z = x$$

f es pues un monomorfismo.

Ejemplo. Sean $A = (\mathbf{Z}, +, 0)$ y $B = \{z / z \in \mathbf{C} \text{ y } |z| = 1\}$. Sea r un número real. La aplicación $M : A \to B$ definida por

$$M : n \to \cos(2\pi rn) + i \cdot \operatorname{sen}(2\pi rn)$$

es un morfismo de $\mathbf{Z}$ en el grupo multiplicativo de números complejos de módulo 1. En efecto, ¡ la validez de

$$M(n + n') = M(n) \cdot M(n')$$
$$\text{si } n, n' \in Z$$

no es otra cosa que el Teorema de De Moivre!.

Afirmación. M es un monomorfismo si, y sólo si, $r \notin \mathbf{Q}$ (o sea, si r es irracional).

Utilizando la proposición anterior, M es un monomorfismo si, y sólo si, $Nu(M) = \{0\}$. Entonces

$$\begin{aligned} 0 \neq n \in Nu(M) &\Leftrightarrow \cos(2\pi rn) + i \cdot \operatorname{sen}(2\pi rn) = 1 \\ &\Leftrightarrow \cos(2\pi rn) = 1 \text{ y } \operatorname{sen}(2\pi rn) = 0 \\ &\Leftrightarrow \text{Existe } k \in \mathbf{Z} \text{ tal que} \\ &\qquad 2\pi rn = 2k\pi \\ &\Leftrightarrow \text{Existe } k \in \mathbf{Z} \text{ tal que} \\ &\qquad r = k/n \\ &\Leftrightarrow r \in \mathbf{Q} \end{aligned}$$

Queda probada nuestra afirmación.

Ejercicios

1. Probar que si n y m son enteros y $r = n/m$ (fracción irreducible), entonces $Nu(M)$ = totalidad de múltiplos enteros de m.

2. Probar que un grupo A es conmutativo si, y sólo si, la aplicación $a \to a^2$ de A en sí misma es un morfismo.

C. Subgrupos

Sean $A = (A, *, e)$ un monoide con identidad y C un subconjunto de A.

Definición. Diremos que * define sobre C una estructura de subgrupo, o simplemente que C es subgrupo de A, si

s1) C es subsemigrupo de A.
s2) $e \in C$.
s3) (C, *, e) es un grupo.

En particular, subgrupo de un semigrupo y subgrupo de un grupo se refieren a los subgrupos de los monoides correspondientes. Conviene notar sin embargo la siguiente proposición.

Proposición. Sea A = (A, *, e) un semigrupo con identidad. Entonces si C es un subconjunto de A, las dos proposiciones siguientes son equivalentes:

i. C es subgrupo de A.
ii. C es submonoide de A y para todo $c \in C$, c' existe y pertenece a C.

Demostración

i. $\Rightarrow$ ii. Es consecuencia de la definición de subgrupo.
ii. $\Rightarrow$ i. Debe verificarse las condiciones s1), s2) y s3) de la definición de subgrupo.

s1) Siendo C un submonoide resta probar que, cualesquiera que sean $u, v, w \in C$, es válida la asociatividad

$$u * (v * w) = (u * v) * w \qquad \text{(o)}$$

Pero, siendo A por hipótesis un semigrupo, (o) es válida cualesquiera que sean u, v, w en A y, en particular, es válida en C.

s2) Siendo C un submonoide es $C \neq \phi$, por lo tanto sea $c \in C$. Entonces $c' \in C$ y también $e = c * c' \in C$.

s3) De acuerdo con s1) y s2) C es un semigrupo con identidad y todo elemento de C es inversible. Entonces C es un grupo.

La implicación ii $\Rightarrow$ i queda probada y con ello la proposición.

Proposición. Sea A = (A, *, e) un grupo. Entonces si C es un subconjunto de A las proposiciones siguientes son todas equivalentes entre sí:

j. C es subgrupo de A.
jj. C es submonoide de A y $c \in C$ implica $c' \in C$.
jjj. $C \neq \phi$ y $x, y \in C \Rightarrow x * y' \in C$.
jv. $C \neq \phi$ y $x, y \in C \Rightarrow x' * y \in C$.

Demostración

j. $\Rightarrow$ jj. Es consecuencia de la definición de subgrupo.
jj. $\Rightarrow$ j. Es caso particular de la misma implicación en la

proposición anterior. Nótese que siendo ahora A un grupo la existencia de c' es automática.

jj. ⇒ jjj. Es inmediata.

jj. ⇒ jv. Es inmediata.

jjj. ⇒ jj. Probemos que C es submonoide de A. Es $\neq \phi$ por jjj. Sea $c \in C$. Entonces aplicando jjj a la situación $x = y = c$ resulta $e = c * c' \in C$. Y aplicando jjj a la situación $x = e$, $y = c$, se tiene $c' = e * c' \in C$. Se ha probado pues que $c \in C$ implica $c' \in C$. Sean $c, t \in C$. Vamos a probar que $c * t \in C$. Sabemos que $t' \in C$. Aplicando jjj a la situación $x = c$, $y = t'$, y sabiendo que $(t')' = t$, resulta

$$c * t = c * (t')' \in C$$

Queda pues probada la implicación.

jv. ⇒ jj. Análoga demostración.

En definitiva, hemos probado las implicaciones

$$\begin{array}{ccccc} j. & \Rightarrow & jj. & \Rightarrow & j. \\ jj. & \Rightarrow & jjj. & \Rightarrow & jj. \\ jj. & \Rightarrow & jv. & \Rightarrow & jj. \end{array}$$

Queda pues probada la proposición.

<u>Ejercicio</u>. Sea A un grupo y sea B un monoide con elemento identidad. Sea $f : A \to B$ un morfismo. Demuestre que

a) Nu (f) es subgrupo de A.
b) Im (f) es subgrupo de B.

Ejemplos

1. Sea X un conjunto no vacío y sea $x_0 \in X$. Sea A = Tran (X) el grupo de transformaciones de X. Sea $C \subset$ Tran (X) definido por

$$f \in C \text{ si, y sólo si, } f(x_0) = x_0$$

Probemos que C es un subgrupo de Tran(X). Utilicemos jj de la proposición anterior.

$C \neq \phi$. En efecto, $id_X \in$ Tran (X) satisface $id_X(x_0) = x_0$, por lo tanto $id_X \in C$.

Sea $g \in C$, o sea $g(x_0) = x_0$. Ahora $g' \in$ Tran (X) satisface

$$g' \circ g = id_X$$

por lo tanto

$$g'(x_0) = g'(g(x_0)) = (g' \circ g)(x_0) = x_0$$

es decir $g' \in C$.

Finalmente, si $f, h \in C$, se tiene

$$(f \circ h)(x_0) = f(h(x_0)) = f(x_0) = x_0$$

de manera que $f \circ h \in C$. Se ha probado que C es un submonoide de Tran (X) y, además, que $g \in C$ implica $g' \in C$, es decir la condición jj.

El lector desarrollará, a modo de ejercicio, el siguiente ejemplo de tipo general. Sea Y un subconjunto no vacío de X. Sea C la totalidad de las $f \in$ Tran(X) tales que

$$f(Y) = Y \text{ o sea}$$
$$\begin{cases} y \in Y \Rightarrow f(y) \in Y \\ y \in Y \Rightarrow y = f(x) \text{ con } e \in Y \end{cases}$$

Demuestre que C es un subgrupo de Tran (X).

2. Sea $A = (\mathbf{Z}, +, 0)$. Sea n_0 un número entero. La totalidad C de múltiplos de n_0, o sea

$$C = \{m / m \in \mathbf{Z} \text{ y } m = r \cdot n_0 \text{ con } r \in Z\}$$

es un subgrupo de **Z**. En efecto, utilicemos jjj. Es claro que $n_0 \in C$, dado que $n_0 = 1 \cdot n_0$. Por lo tanto, $C \neq \phi$. Además, si m_1 y $m_2 \in C$ podemos escribir $m_1 = r_1 \cdot n_0$ y $m_2 = r_2 \cdot n_0$, por lo tanto

$$m_1 - m_2 = (r_1 - r_2) \cdot n_0$$

o sea

$$m_1 - m_2 \in C$$

C es pues un subgrupo de **Z**.

Recíprocamente, sea C un subgrupo de $(\mathbf{Z}, +, 0)$. Si $C \neq 0$ existe $c \in C$, $0 \neq c$. Por lo tanto, $-c \in C$ (en virtud de jj). O sea que c y -c pertenecen a C. Esto implica que C contiene al menos un entero positivo. O sea

$$C \cap N \neq \phi$$

Siendo $C \cap \mathbf{N}$ un subconjunto no vacío de **N**, existe $m \in C \cap \mathbf{N}$ tal que

$$h \in C \cap \mathbf{N} \Rightarrow m \leq h$$

(o sea, m es el primer elemento de $C \cap \mathbf{N}$). Es claro que $m \in C$.

Sea ahora $t \in C$. En virtud del algoritmo de división en **Z** existen $u, v \in \mathbf{Z}$ tales que

$$t = u \cdot m + v, \text{ donde}$$
$$(:) \qquad 0 \leq v < m$$

Por lo tanto

$$v = t - u \cdot m \in C \text{ puesto que } t \in C \text{ y } u \cdot m \in C$$

Ahora, si $v \neq 0$, se sigue de (:) que $v \in C \cap \mathbf{N}$, lo que es un absurdo dada la mínima expresión de m. Por lo tanto se ha probado que

$$c \in C \Rightarrow c \text{ es múltiplo de } m$$

Reuniendo los dos resultados se tiene que: "C es un subgrupo de **Z** si, y sólo si, existe $m \in$ **Z**, $0 \leq m$ tal que C es la totalidad de múltiplos enteros de m". Se suele escribir C = (m) y se dice que C es el subgrupo de **Z** generado por m.

3. Sea A un monoide y sea Aut (A) el grupo de automorfismos de A. Entonces Aut(A) es un subgrupo de End(A), según se infiere de la definición de subgrupo.

4. Sea A un monoide y sea Int (A) la totalidad de automorfismos interiores de A. Entonces Int(A) es un subgrupo de Aut(A). En efecto, recordemos primeramente que $g \in$ Int (A) si, y sólo si, existe $u \in A$ tal que $g(a) = u * a * u'$. Ya vimos que Int (A) es submonoide de Aut (A). Probemos (según jj) que $g \in$ Int (A) implica que $g' \in$ Int (A). Pero esto es inmediato dado que si

$$g(a) = u * a * u', \quad a \in A$$

entonces

$$g'(a) = u' * a * u$$

5. Sea (A, *, e) un semigrupo. Sea U (A) el subsemigrupo de elementos inversibles de A. Entonces U (A) es un subgrupo de A.

D. Relaciones de Equivalencia en Un Grupo

Sea G = (G, *, e) un grupo. Sea $\sim$ una relación de equivalencia definida por G. Recordemos que $\sim$ "distingue" pares de elementos de G de acuerdo con las siguientes reglas: $(x, y, z \in G)$

$x \sim x$

Si $x \sim y$ entonces $y \sim x$

Si $x \sim y$ e $y \sim z$ entonces $x \sim z$

La introducción de una relación de equivalencia dentro del grupo G, sin una motivación al respecto, podría tal vez desorientar al lector. Sin entrar en mayores detalles digamos ahora que el estudio de "ciertas" relaciones de equivalencia en un grupo G permite determinar todos los grupos G', que son imágenes de G por morfismo. Por ejemplo, aplicado eso al grupo G = (**Z**, +, 0) es posible construir la familia más importante de grupos conmutativos finitos, a saber: los grupos cíclicos. Comencemos primeramente aclarando aquéllo de "ciertas" relaciones de equivalencia. $\sim$ denota, como arriba, una relación de equivalencia sobre G.

Definición. Se dice que $\sim$ es compatible a la izquierda (con la estructura de grupo de G) si

$$a \sim b \Rightarrow x * a \sim x * b$$

cualquiera que sea $x \in G$.

Definición. Se dice que $\sim$ es compatible a la derecha (con la estructura de grupo de G) si

$$a \sim b \Rightarrow a * x \sim b * x$$

cualquiera que sea $x \in G$.

Definición. Se dice que $\sim$ es compatible (con la estructura de grupo de G) si $\sim$ es compatible a la izquierda y a la derecha. Por supuesto que en el caso de ser G conmutativo no es necesario hacer distinción alguna.

Ejemplo. La siguiente relación definida en **Q**:

$$a \sim b \text{ si, y sólo si, } a^2 = b^2$$

es de equivalencia, como el lector podrá verificar fácilmente.

i. $\sim$ es compatible con la estructura de ($Q\#$, ., 1).
En efecto, sea $a \sim b$ y sea $x \in Q\#$. Entonces

$$(x \cdot a)^2 = x^2 \cdot a^2 = x^2 \cdot b^2 = (x \cdot b)^2$$

de manera que

$$x . a \sim x . b$$

y por la conmutatividad de $Q\#$

$$a \cdot x \sim b \cdot x$$

ii. $\sim$ no es compatible con la estructura de (**Q**, +, 0).
En efecto,

$$1 \sim -1$$

sin embargo, es falso que

$$1 + 1 \sim 1 + (-1)$$

Ejemplo. Sea $X = \{1, 2, 3\}$ y sea G = Tran(X) = el grupo de transformaciones de X. Sea $\sim$ la siguiente relación definida sobre G

$$f \sim g \text{ si, y sólo si, } f(1) = g(1)$$

Es fácil comprobar que $\sim$ es una relación de equivalencia. Estudiemos la compatibilidad de $\sim$ respecto de la estructura de G.

i. $\sim$ es compatible a la izquierda. En efecto, sea $f \sim g$ y sea $h \in G$. Entonces $f(1) = g(1)$ y consecuentemente

$$(h \circ f)(1) = h(f(1)) = h(g(1)) = (h \circ g)(1)$$

por lo tanto

$$h \circ f \sim h \circ g$$

ii. $\sim$ no es compatible a la derecha. En efecto, sean $f, g, h \in G$ definidos por

$$f(1) = 2,\ f(2) = 1,\ f(3) = 3$$
$$g(1) = 2,\ g(2) = 3,\ g(3) = 1$$
$$h(1) = 3,\ h(2) = 2,\ h(3) = 1$$

por lo tanto

$$f \sim g$$

Sin embargo

$$(f \circ h)(1) = f(h(1)) = f(3) = 3$$
$$(g \circ h)(1) = g(h(1)) = g(3) = 1$$

lo cual prueba nuestra afirmación.

Proposición. Sea G un grupo y sea $\sim$ una relación de equivalencia definida sobre G. Entonces $\sim$ es compatible si, y sólo si,

(i) $$a \sim b \text{ y } c \sim d \Rightarrow a * c \sim b * d$$

Demostración. Sea $\sim$ compatible, sean $a \sim b$ y $c \sim d$. Entonces

$$a \sim b \Rightarrow a * c \sim b * c$$
$$a \sim d \Rightarrow b * c \sim b * d$$

por lo tanto, por transitividad,

$$a * c \sim b * d$$

lo cual prueba la primera parte.

Recíprocamente sea (i) válida. Entonces, si $a \sim b$ y $x \in G$ resulta, aplicando (i) a las situaciones,

$$a \sim b \text{ y } x \sim x$$
$$x \sim x \text{ y } a \sim b$$

las relaciones buscadas

$$a * x \sim b * x$$
$$x * a \sim x * b$$

con lo que queda probada la proposición.

El siguiente teorema caracteriza las relaciones de equivalencia compatibles a la izquierda en términos de subgrupos y demuestra también recíprocamente que todo subgrupo da lugar a una relación de equivalencia de compatible. Después del teorema comprobaremos que un objeto determina el otro unívocamente.

Teorema. Sea G un grupo. Entonces

1) Si $\sim$ es una relación de equivalencia compatible a la izquierda, el subconjunto $H_\sim$ de G definido por

$$H_\sim = \{a \,/\, a \sim e\} = \{a \,/\, e \sim a\}$$

es un subgrupo de G que satisface

$$a \sim b \Leftrightarrow b' * a \in H_\sim$$

Recíprocamente

2) Si H es un subgrupo de G entonces la relación

(_) $$a \approx b \Leftrightarrow b' * a \in H$$

es una relación de equivalencia sobre G compatible a la izquierda.

Demostración

1. $H_\sim$ es no vacío dado que $e \sim e$ implica $e \in H_\sim$. Sean $x, v \in H_\sim$, entonces $x \sim e$ y $e \sim v$ de manera que $x \sim v$. Pero utilizando la compatibilidad a la izquierda de $\sim$ resulta

$$v' * x \sim e$$

con lo que $v' * x \in H_\sim$. Utilizando jv de la Sección 3 se tiene que $H_\sim$ es subgrupo de G. Además, en virtud de la compatibilidad a la izquierda de $\sim$

$$a \sim b \Leftrightarrow b' * a \sim e \Leftrightarrow b' * a \in H$$

lo cual demuestra la segunda parte de 1).

2. Sea $\approx$ la relación definida por (_). Debemos probar que $\approx$ es de equivalencia compatible a la izquierda. $\approx$ es de equivalencia:

- $x' * x = e \in H \Rightarrow x \approx x$
- $x \approx y \Rightarrow y' * x \in H \Rightarrow (y' * x)' = x' * y \in H \Rightarrow y \approx x$
- $x \approx y$ e $y \approx z \Rightarrow y' * x \in H$ y $z' * y \in H \Rightarrow (z' * y) * (y' * x) = z' * x \in H \Rightarrow x \approx z$

lo cual demuestra nuestra afirmación (nótese que en los tres pasos se ha utilizado la propiedad de ser H un subgrupo de G). $\approx$ es compatible a la izquierda:

$$a \approx b \Rightarrow b' * a \in H$$
$$\Rightarrow (x * b)' * (x * a) = b' * x * x' * a = b' * a \in H$$
$$\Rightarrow x * a \approx x * b$$

queda pues probado el teorema.

El teorema anterior asocia entonces a una relación de equivalencia compatible a la izquierda $\sim$ un subgrupo $H_\sim$ de G:

(1) $$\sim \;\rightarrow\; H_\sim$$

y asocia a todo subgrupo H de G una relación de equivalencia compatible a la izquierda $\approx$ sobre G:

(2) $$H \rightarrow \approx$$

Por tanto, si se denota con $\mathbf{E}_1$ la totalidad de relaciones de equivalencia sobre G compatibles a la izquierda y con $\mathbf{S}$ la totalidad de subgrupos de G, entonces (1) y (2) definen aplicaciones

(1') $\qquad \underline{O} : \mathbf{E}_1 \to \mathbf{S}$

(2') $\qquad \underline{U} : \mathbf{S} \to \mathbf{E}_1$

Interesa aquí ver cómo las composiciones de $\underline{O}$ y $\underline{U}$ satisfacen

$$\underline{O} \circ \underline{U} = id_{\mathbf{S}}$$
$$\underline{U} \circ \underline{O} = id_{\mathbf{E}_1}$$

o, en palabras, que si partimos de un subgrupo H de G y le asociamos la relación de equivalencia correspondiente según (2), y luego a ésta última le asociamos el subgrupo correspondiente de acuerdo con (1), volvemos a obtener H. Análogamente, si partimos de una relación de equivalencia compatible a la izquierda $\sim$ y le asociamos el subgrupo correspondiente según (1), y luego a éste último le asociamos la relación de equivalencia de acuerdo con (2), volvemos a obtener $\sim$. De esta forma se obtiene una biyección natural entre el conjunto $\mathbf{S}$ y el conjunto $\mathbf{E}_1$.

Sea $\sim$ una relación de equivalencia compatible a la izquierda y sean

$$\underline{O} : \sim \;\to H_{\sim}$$
$$\underline{U} : H_{\sim} \to \approx$$

vamos a probar que $\sim \; = \; \approx$, o sea que

$$x \sim y \text{ si, y sólo si, } x \approx y$$

Nótese que de acuerdo con el teorema anterior

$$H_{\sim} = \{a / a \sim e\}$$
$$x \approx y \Leftrightarrow y' * x \in H_{\sim}$$

Pero por 1) del mismo teorema

$$x \sim y \Leftrightarrow y' * x \in H$$

Por lo tanto

$$x \sim y \Leftrightarrow x \approx y$$

o sea

$$\sim \; = \; \approx$$

lo cual prueba nuestra afirmación, o sea $\underline{U} \circ \underline{O} = id_{\mathbf{E}_1}$.

Sea ahora H un subgrupo de G y sean

$$\underline{U} : H \to \approx$$
$$\underline{O} : \approx \;\to H_{\approx}$$

Vamos a probar que $H = H_{\approx}$. De acuerdo con el teorema anterior se tiene

$$x \approx y \Leftrightarrow y' * x \in H$$
$$H_{\approx} = \{a / a \approx e\}$$

$H_{\approx} \subset H$. En efecto, $x \in H_{\approx} \Rightarrow x \approx e$
$\Rightarrow x = e' * x \in H$

$H \subset H_{\approx}$. En efecto, $x \in H \Rightarrow e' * x \in H$
$\Rightarrow x \approx e$
$\Rightarrow x \in H_{\approx}$

De ambas inclusiones resulta la igualdad

$$H = H_{\approx}$$

queda pues probada nuestra afirmación.

Resultados idénticos se obtienen al considerar relaciones de equivalencia compatibles a la derecha. Los resultados son los siguientes.

Si H es subgrupo de G entonces

$$a \sim b \Leftrightarrow a * b' \in H$$

es una relación de equivalencia compatible a la derecha.

Recíprocamente, si $\sim$ es una relación de equivalencia compatible a la derecha entonces

$$H_{\sim} = \{a / a \sim e\}$$

es un subgrupo de G.

Estamos ahora en condiciones de combinar ambos resultados para obtener una caracterización de las relaciones de equivalencia compatibles (a la derecha y a la izquierda) en términos de subgrupos de G.

Teorema.

1) Si $\sim$ es una relación de equivalencia compatible (a la izquierda y a la derecha), entonces el subgrupo asociado H satisface:

(d) $$x \in G \text{ y } h \in H \Rightarrow x * h * x' \in H$$

2) Recíprocamente, si H es un subgrupo de G que satisface la condición (d) entonces la relación de equivalencia asociada

$$x \sim y \Leftrightarrow y' * x \in H$$

es compatible (a la izquierda y a la derecha).

Demostración

1. Sean $x \in G$ y $h \in H$. Entonces por la definición de H es

$$h \sim e$$

Por la compatibilidad a la izquierda de $\sim$ resulta

$$x * h \sim x$$

y por la compatibilidad a la derecha de $\sim$

$$x * h * x' \sim e$$

o sea

$$x * h * x' \in H$$

como queríamos probar.

2. Sea H un subgrupo de G que satisface (d). Entonces por el teorema anterior

$$x \sim y \Leftrightarrow y' * x \in H$$

es una relación de equivalencia compatible a la izquierda. Debemos probar que es también compatible a la derecha. Sea pues

$$a \sim b \text{ y } x \in G$$

Entonces

$$b' * a \in H$$

y por lo tanto

$$x' * (b' * a) * x = x' * (b' * a) * (x')' \in H$$

o sea

$$(b * x)' * (a * x) = (x' * b') * (a * x) \in H$$

o sea, finalmente,

$$a * x \sim b * x$$

que es la compatibilidad a la derecha pedida.

Definición. Se denomina subgrupo distinguido† de G a todo subgrupo H que satisface la condición (d) del teorema anterior.

Ejemplos

1. Sea G un grupo. Entonces

$$H = G \text{ y } H = \{e\}$$

son subgrupos distinguidos de G y se les denomina subgrupos distinguidos triviales.

2. Sea G un grupo conmutativo. Todo subgrupo de G es entonces distinguido.

3. Sea X = {1, 2, 3} y sea G = Tran(X). El subgrupo

$$H = \{f \,/\, f(1) = 1\}$$

no es distinguido. En efecto, la relación de equivalencia

$$f \sim g$$

asociada a H es

† Se denomina también subgrupo invariante o subgrupo normal.

$$
\begin{aligned}
f \sim g &\Leftrightarrow g' \circ f \in H \\
&\Leftrightarrow (g' \circ f)(1) = 1 \\
&\Leftrightarrow g'(f(1)) = 1 \\
&\Leftrightarrow f(1) = g(1)
\end{aligned}
$$

y ya se demostró que esta relación de equivalencia es compatible a la izquierda pero no a la derecha.

4. Sea **Z** = (**Z**, +, 0). Vamos a determinar todas las relaciones de equivalencia compatibles con la estructura de grupo de **Z** (o también, simplemente dicho, compatibles con +).

Siendo **Z** un grupo conmutativo todos sus subgrupos son invariantes. Los subgrupos de **Z** están caracterizados como sigue:

H es subgrupo de **Z** si, y sólo si, existe $m \in \mathbf{Z}$, $0 \leq m$ tal que

$$
\begin{aligned}
H &= \{r \cdot m \,/\, r \in \mathbf{Z}\} \\
&= \text{totalidad de múltiplos enteros de } m.
\end{aligned}
$$

Sea entonces $\sim$ una relación de equivalencia en **Z** compatible. Sea H el subgrupo asociado a $\sim$. Por lo anteriormente dicho existe $m \in Z$, $0 \leq m$ tal que H es la totalidad de múltiplos enteros de m. Entonces

$$a \sim b \Leftrightarrow a - b \in H$$

Por lo tanto, si $H = 0$

$$a \sim b \Leftrightarrow a = b$$

y si $H \neq 0$, entonces $m \neq 0$ con lo que

$$a \sim b \Leftrightarrow a - b \text{ es divisible por } m.$$

Este tipo de relación de equivalencia no es otra cosa que la relación de congruencia módulo m estudiada en aritmética y que se denota por $a \equiv b \mod (m)$. Se ha probado pues que las relaciones de equivalencia en **Z** compatibles con + son:

- la igualdad, y
- las congruencias mod(m), $0 < m$.

E. Grupo Cociente de Un Grupo por Un Subgrupo Distinguido

Sea G un grupo y sea $\sim$ una relación de equivalencia definida sobre G. Por la teoría de relaciones de equivalencia sabemos que a G y $\sim$ está asociado un conjunto denotado por

$$G/\sim \,:\, \text{el conjunto cociente de } G \text{ por } \sim$$

y una aplicación

$$g : G \to G/\sim \,:\, \text{la aplicación canónica de } G \text{ en } G/\sim.$$

Recordemos sus definiciones:

$G/\sim$ es el conjunto de clases de equivalencia de G por $\sim$, o sea en símbolos $U \in G/\sim$ si, y sólo si, $U \subset G$ y existe $u \in G$ tal que

$$U = \{x / x \sim u\}$$

$\mathcal{g}$ es la aplicación definida por $u \to \{x / x \sim u\}$.

Problema. **Definir una Estructura de Grupo en $G/\sim$ que Convierta A $\mathcal{g} : G \to G/\sim$ en Morfismo de Grupos.**

En esta sección vamos a resolver este problema, cuya solución puede, sin duda, considerarse como una pieza clave dentro de la teoría de estructuras algebraicas.

Teorema Fundamental. Sea G un grupo y sea $\sim$ una relación de equivalencia definida sobre G y compatible (a la izquierda y a la derecha) con la estructura de grupo de G. Sea $G/\sim$ el conjunto cociente de G por $\sim$ y sea $\mathcal{g} : G \to G/\sim$ la aplicación canónica de G sobre $G/\sim$. Entonces:

1) Existe una única estructura de grupo sobre $G/\sim$ que convierte a $\mathcal{g}$ en un morfismo de grupos.

2) $Nu(\mathcal{g})$ = el subgrupo distinguido asociado a $\sim$.

Demostración

1. Sean S y $T \in G/\sim$. Existen entonces s y $t \in G$ tales que

$$S = \{x / x \sim s\} = \mathcal{g}(s)$$
$$T = \{x / x \sim s\} = \mathcal{g}(t)$$

Afirmación. $\mathcal{g}(s * t)$ está unívocamente determinado por S y T, o sea que si $s, s_1 \in S$ y $t, t_1 \in T$ entonces

$$\mathcal{g}(s * t) = \mathcal{g}(s_1 * t_1)$$

En efecto,

$$s, s_1 \in S \Rightarrow s \sim s_1$$
$$t, t_1 \in T \Rightarrow t \sim t_1$$

y por ser $\sim$ compatible

$$s * t \sim s_1 * t_1$$

de manera que

$$\mathcal{g}(s * t) = \mathcal{g}(s_1 * t_1)$$

con lo cual queda probada nuestra afirmación.

En virtud del resultado precedente vamos a asociar

(") $$(S, T) \to S * T = \mathcal{g}(s * t) \quad \text{donde } s \in S \text{ y } t \in T$$

De esta manera queda definida sobre $G/\sim$ una ley de composición interna que convierte a $G/\sim$ en un monoide $(G/\sim, *)$.

Probemos ahora que $\mathcal{g} : G \to G/\sim$ es un morfismo de los monoides correspondientes. Esto es una consecuencia de la definición (''). En efecto, sean $s, t \in G$ entonces $\mathcal{g}(s)$ y $\mathcal{g}(t) \in G/\sim$ y según ('') la definición de $\mathcal{g}(s) * \mathcal{g}(t)$ es

$$\mathcal{g}(s) * \mathcal{g}(t) = \mathcal{g}(s * t)$$

dado que $s \in \mathcal{g}(s)$ y $t \in \mathcal{g}(t)$. Por lo tanto $\mathcal{g}$ es un morfismo. Además, siendo $\mathcal{g}$ una aplicación sobre, $\mathcal{g}$ es un morfismo sobre. Como tal transporta la estructura de grupo de G sobre $G/\sim$. Así, por ejemplo, si $S \in G/\sim$ y $S = \mathcal{g}(s)$, llamando entonces $\underline{e} = \mathcal{g}(e)$

$$\underline{e} * S = \mathcal{g}(e) * \mathcal{g}(s) = \mathcal{g}(e * s) = \mathcal{g}(s) = S$$
$$S * \underline{e} = \mathcal{g}(s) * \mathcal{g}(e) = \mathcal{g}(s * e) = \mathcal{g}(s) = S$$

de manera que $\underline{e}$ es elemento identidad de $(G/\sim, *)$. Queda pues probada la existencia de una estructura de grupo sobre $G/\sim$ que convierte a $\mathcal{g}$ en un morfismo.

Pasemos ahora a considerar la cuestión de unicidad. Sea $(G/\sim, \circledast)$ otra estructura de monoide sobre $G/\sim$ que convierte a $\mathcal{g}$ en un morfismo. Entonces si $S, T \in G/\sim$ y $\mathcal{g}(s) = S$, $\mathcal{g}(t) = T$ se tiene

$$S \circledast T = \mathcal{g}(s) \circledast \mathcal{g}(t) = \mathcal{g}(s * t) = \mathcal{g}(s) * \mathcal{g}(t) = S * T$$

lo cual demuestra que $* = \circledast$ Esto concluye la demostración de 1.

2. Ya se ha visto que el elemento identidad de $(G/\sim, *)$ es $\underline{e} = \mathcal{g}(e)$.

$$\begin{aligned} s \in Nu(\mathcal{g}) &\Leftrightarrow \mathcal{g}(s) = \underline{e} = \mathcal{g}(e) \\ &\Leftrightarrow s \sim e \\ &\Leftrightarrow s \in H_\sim = \{x / x \sim e\} \end{aligned}$$

por lo tanto

$$Nu(\mathcal{g}) = H_\sim .$$

El teorema queda así probado.

Definición. Con la notación del teorema anterior, $G/\sim$ se denomina el grupo cociente de G por la relación de equivalencia $\sim$. Al morfismo $\mathcal{g} : G \to G/\sim$ se le denomina morfismo canónico. Si H es un subgrupo distinguido de G, se designa G/H al grupo cociente $G/\sim$ de G por la relación de equivalencia de G asociada a H.

Ejemplo. Sea G un grupo y sea $H = \{e\}$ el subgrupo formado por el elemento identidad de G. La relación de equivalencia asociada a H es la siguiente:

$$\begin{aligned} a \sim b &\Leftrightarrow b' * a \in H = \{e\} \\ &\Leftrightarrow b' * a = e \\ &\Leftrightarrow a = b \end{aligned}$$

es decir, es la igualdad. Los elementos de $G/\sim$ no son otra cosa que los subconjuntos de G formados por un solo elemento: $\{x\}$,

$x \in G$. La aplicación canónica está definida por

$$\mathfrak{g} : x \to \{x\}$$

La estructura de grupo en $G / \{e\}$ será entonces

$$\{x\} * \{y\} = \{x * y\}$$

Es evidente que $\mathfrak{g}$ es un monomorfismo. Como es también un morfismo sobre, se tiene que $\mathfrak{g}$ es un isomorfismo, por lo tanto

$$\boxed{G/\{e\} \simeq G}$$

Por ejemplo, si $\mathbf{Z}$ es el grupo aditivo de enteros racionales se tiene el isomorfismo : $\mathbf{Z} / \{0\} \simeq \mathbf{Z}$.

Como complemento del anterior se tiene el teorema siguiente.

Teorema. Sea G un grupo y sea H un subgrupo de G. Entonces las siguientes condiciones son equivalentes entre sí

d1) H es subgrupo distinguido de G.
d2) Existe un grupo L y un morfismo $f : G \to L$ tal que

$$Nu(f) = H$$

Demostración

d1) $\Rightarrow$ d2).

Sea G / H el grupo cociente de G por (la relación de equivalencia asociada a) el subgrupo distinguido H. Si $\mathfrak{g}$ denota el morfismo canónico, se sigue del punto 2 del teorema anterior que $H = Nu(\mathfrak{g})$.

d2) $\Rightarrow$ d1).

Sea L un grupo y sea $f : G \to L$ un morfismo tal que $H = Nu(f)$. Entonces si $h \in H$ y $x \in G$ se tiene

$$\begin{aligned} f(x * h * x') &= f(x) * f(h) * f(x') \\ &= f(x) * e * f(x') \\ &= f(x) * f(x') = f(x) * f(x)' \\ &= e \end{aligned}$$

de manera que

$$x * h * x' \in H$$

lo cual muestra que H es subgrupo distinguido.

Ejemplos

1. Grupos cocientes de $\mathbf{Z} = (\mathbf{Z}, +, 0)$. Sea $0 < m$, $m \in \mathbf{Z}$. Se estudiará el grupo cociente de $\mathbf{Z}$ por el subgrupo denotado por (m) de múltiplos enteros de m. La relación de equivalencia sobre $\mathbf{Z}$ asociada a (m) es

$$a \sim b \text{ si, y sólo si, } m \text{ divide a } a - b$$

Sea $k \in \mathbf{Z}$. En virtud del algoritmo euclidiano de división en $\mathbf{Z}$ existen $q, r \in \mathbf{Z}$ tales que

$$k = m \cdot q + r, \; 0 \leq r < m$$

estando q y r unívocamente determinados por estas dos propiedades. El resto de la división de k por m se denomina r. Resulta inmediatamente que

$$k \sim r$$

lo cual demuestra que todo elemento de **Z** es congruente a uno y sólo uno de los enteros r que satisfacen

$$0 \leq r < m$$

a saber: su resto de la división por m.

Por consecuencia, $\mathbf{Z} / \sim$ consta exactamente de m clases de equivalencia a saber

$$\begin{aligned} \underline{0} &= \{k / k \sim 0\} \\ \underline{1} &= \{k / k \sim 1\} \\ &\cdots\cdots\cdots\cdots \\ \underline{m-1} &= \{k / k \sim m-1\} \end{aligned}$$

Utilizando el morfismo canónico $\mathfrak{g} : \mathbf{Z} \to \mathbf{Z}/\sim$, $\mathfrak{g}(k) = r$, donde r denota el resto de la división en **Z** de k por m, así se tiene que

$$\begin{aligned} \underline{0} &= \mathfrak{g}(0) \\ \underline{1} &= \mathfrak{g}(1) \\ &\cdots\cdots \\ \underline{m-1} &= \mathfrak{g}(m-1) \end{aligned}$$

Veamos la estructura de grupo en $\mathbf{Z} / \sim$. De acuerdo con su definición si s, t denotan enteros que satisfacen $0 \leq s < m$, $0 \leq t < m$ y $\underline{s}$, $\underline{t}$ las clases correspondientes en $\mathbf{Z} / \sim$ se tendrá

$$\begin{aligned} \underline{s} + \underline{t} &= \mathfrak{g}(s + t) \\ &= \underline{r} \end{aligned}$$

donde r denota el resto de la división de s + t por m.

Fijemos las ideas con ejemplos concretos.
Sea m = 5. Entonces $\mathbf{Z} / (5)$ consta de los 5 elementos

$\underline{0} = \{k / k \sim 0\}$ = múltiplos de 5
$\underline{1} = \{k / k \sim 1\}$ = enteros cuya división por 5 da resto 1
$\underline{2} = \{k / k \sim 2\}$ = enteros cuya división por 5 da resto 2
$\underline{3} = \{k / k \sim 3\}$ = enteros cuya división por 5 da resto 3
$\underline{4} = \{k / k \sim 4\}$ = enteros cuya división por 5 da resto 4

La estructura de grupo de $\mathbf{Z} / (5)$ está dada por la tabla:

+	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$	$\underline{4}$
$\underline{0}$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$	$\underline{4}$
$\underline{1}$	$\underline{1}$	$\underline{2}$	$\underline{3}$	$\underline{4}$	$\underline{0}$
$\underline{2}$	$\underline{2}$	$\underline{3}$	$\underline{4}$	$\underline{0}$	$\underline{1}$
$\underline{3}$	$\underline{3}$	$\underline{4}$	$\underline{0}$	$\underline{1}$	$\underline{2}$
$\underline{4}$	$\underline{4}$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$

donde, por ejemplo, $\underline{3} + \underline{4} = \underline{2}$, pues 2 es el resto de la división de 3 + 4 por 5, etc..

Sea m = 6. Una discusión análoga a las precedentes permite obtener la siguiente estructura sobre Z / (6):

+	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$	$\underline{4}$	$\underline{5}$
$\underline{0}$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$	$\underline{4}$	$\underline{5}$
$\underline{1}$	$\underline{1}$	$\underline{2}$	$\underline{3}$	$\underline{4}$	$\underline{5}$	$\underline{0}$
$\underline{2}$	$\underline{2}$	$\underline{3}$	$\underline{4}$	$\underline{5}$	$\underline{0}$	$\underline{1}$
$\underline{3}$	$\underline{3}$	$\underline{4}$	$\underline{5}$	$\underline{0}$	$\underline{1}$	$\underline{2}$
$\underline{4}$	$\underline{4}$	$\underline{5}$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$
$\underline{5}$	$\underline{5}$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$	$\underline{4}$

2. Grupo cociente de **Q** por el subgrupo **Z** : **Q** / **Z**. **Q** denota entonces el grupo aditivo de números racionales y **Z** el subgrupo de enteros racionales. Este último determina sobre **Q** la siguiente relación de equivalencia

$$x \sim y \Leftrightarrow x - y \in \mathbf{Z}$$

Sea **Q** / **Z** el grupo cociente y sea $\mathfrak{g} : \mathbf{Q} \to \mathbf{Q} / \mathbf{Z}$ el morfismo canónico. Adoptaremos la siguiente notación para designar los elementos de **Q** / **Z**

$$\mathfrak{g}(p / q) = [p / q]$$

La estructura de grupo en **Q** / **Z** está dada entonces por

$$[p / q] + [r / s] = [(ps + qr) / qs]$$

Veamos algunas propiedades de este grupo cociente

a) **Q** / **Z** es un grupo infinito.

En efecto, sea

$$p_1, p_2, \dots, p_i, \dots$$

cualquier conjunto infinito de números enteros positivos primos. Sean éstos dados en el orden natural en Z:

$$p_1 < p_2 < \dots$$

afirmamos entonces que $[1/p_i] \neq [1/p_j]$ si $i \neq j$. Esta afirmación implicará la infinitud de **Q** / **Z**. Hagamos la demostración para el caso $i = 1$, $j = 2$. Entonces si

$$[1 / p_1] = [1 / p_2]$$

se tendrá

$$1 / p_1 - 1 / p_2 = n \in \mathbf{Z}$$

por lo tanto

$$0 < p_2 - p_1 = n \cdot p_1 \cdot p_2$$

pero esto es un absurdo, pues afirma que $p_2 - p_1$ es divisible por p_2 y $0 < p_2 - p_1 < p_2$. Nuestra afirmación queda probada.

b) Para todo $x \in \mathbf{Q}/\mathbf{Z}$ existe $n \in \mathbf{N}$ tal que $nx = \underbrace{x + x + \ldots + x}_{n \text{ veces}} = 0$

En efecto, si $x \in \mathbf{Q}/\mathbf{Z}$ existe $p/q \in \mathbf{Q}$ tal que

$$x = [p/q] \quad q \neq 0, \ p, q \in \mathbf{Z}$$

Pero entonces

$$qx = q[p/q] = [q(p/q)] = [p] = 0$$

pues $p \in \mathbf{Z}$

Por lo tanto confirma nuestra afirmación. Esta propiedad se expresa diciendo que $\mathbf{Q}/\mathbf{Z}$ es un grupo de torsión.

F. Un Teorema de Isomorfismo

En esta sección resolveremos el siguiente problema utilizando métodos estudiados previamente.

Problema. Sea G un grupo. Determinar todos los grupos L que sean imágenes de G por morfismos; o sea, determinar todos los grupos L para los cuales existen morfismos sobre $f : G \to L$.

Este problema admite la siguiente solución.

Solución. La clase de grupos $\{L\}$ que son imágenes de G por morfismos "coincide" con la clase $\{G/H\}$ de grupos cocientes de G por subgrupos distinguidos de G. Precisando tenemos:

Teorema. Sean G y L grupos y sea $f : G \to L$ un morfismo sobre. Existe entonces un único subgrupo distinguido H de G y un isomorfismo $g : G/H \to L$ con la propiedad que el diagrama

(D)
$$\begin{array}{ccc} & G & \\ \mathcal{g} \swarrow & & \searrow f \\ G/H & \xrightarrow{g} & L \end{array}$$

es conmutativo, o sea

$$g \circ \mathcal{g} = f$$

($\mathcal{g}$ denota el morfismo canónico).

Nota 1. La conmutatividad del diagrama anterior equivale a decir que L es isomorfo, en forma natural, a un grupo cociente de G.

Nota 2. La coincidencia a que se hace referencia en la solución del problema se obtiene por medio del teorema estableciendo la aplicación

$$L \to G/H$$

Demostración del Teorema. Definimos primeramente

$$H = Nu(f)$$

y siendo éste un subgrupo distinguido formamos el grupo cociente G / H. Vamos ahora a definir un morfismo $G/H \to L$. Sea $S \in G/H$. Existe $s \in G$ tal que $S = \{x / x \sim s\} = \mathcal{G}(s)$. Analicemos el elemento $f(s) \in L$. Si $s_1 \in S$, entonces $s_1 \sim s$, o sea $s' * s_1 \in H = Nu(f)$ de manera que

$$f(s' * s_1) = e$$

y, también, siendo f morfismo

$$e = f(s') * f(s_1) = f(s)' * f(s_1)$$

o sea

$$f(s) = f(s_1)$$

lo cual demuestra que $f(s)$ está unívocamente determinado por S, es decir

$$S \to f(s), \text{ si } s \in S$$

define una aplicación

$$\text{(I)} \qquad \boxed{\begin{array}{c} g : G / H \to L \\ g(S) = f(s) \text{ si } s \in S \end{array}}$$

Vamos a probar que g es un morfismo. Sean $S_1, S_2 \in G / H$. Entonces si $s_1 \in S_1$ y $s_2 \in S_2$ se tiene, en virtud de la definición de $S_1 * S_2$, que

$$s_1 * s_2 \in S_1 * S_2$$

por lo tanto de (I)

$$\begin{aligned} g(S_1 * S_2) &= f(s_1 * s_2) \\ &= f(s_1) * f(s_2) \\ &= g(S_1) * g(S_2) \end{aligned}$$

que muestra bien que g es un morfismo. Nótese además que si $s \in G$ entonces $s \in \mathcal{G}(s)$ y se tiene

$$f(s) = g(\mathcal{G}(s)) = (g \circ \mathcal{G})(s)$$

de manera que

$$f = g \circ \mathcal{G}$$

lo cual prueba la conmutatividad del diagrama (D).

Verifiquemos que g es un isomorfismo.

i. g es un morfismo sobre. En efecto, sea $u \in L$, entonces siendo f un morfismo sobre existe $x \in G$ tal que $f(x) = u$. Por lo tanto de (:) se tiene $u = f(x) = g(\mathcal{G}(x))$ que muestra que g es un morfismo sobre.

ii. g es monomorfismo. Deberá probarse que $Nu(g) = \{e\}$. Sea $S \in Nu(g)$. Entonces si $s \in S$

$$f(s) = g(\mathcal{G}(s)) = g(S) = e$$

por lo tanto $s \in H$. Esto implica $S = H = e$ = identidad de G/H. g es pues un monomorfismo.

Veamos finalmente la cuestión relativa a la unicidad del subgrupo H. Sea, pues, H' un subgrupo distinguido de G y sea $g' : G/H' \to L$ un isomorfismo que hace conmutativo el diagrama

$$\begin{array}{ccc} & G & \\ \mathfrak{g}' \swarrow & & \searrow f \\ G/H' & \xrightarrow[g']{} & L \end{array}$$

Vamos a probar que $H = H'$. En efecto,

$$\begin{aligned} u' \in H' &\Rightarrow f(u') = g'(\mathfrak{g}'(u')) = g'(e) = e \\ &\Rightarrow u' \in H, \text{ o sea } H' \subset H \\ u \in H &\Rightarrow e = f(u) = g'(\mathfrak{g}'(u)) \\ &\Rightarrow \mathfrak{g}'(u) = e \qquad \text{(por ser } g' \text{ un isomorfismo)} \\ &\Rightarrow u \in Nu(\mathfrak{g}') = H', \text{ o sea } H \subset H'. \end{aligned}$$

Es decir, $H = H'$ como deseabamos probar. El teorema queda probado.

Ejemplos

1. Sea G un grupo y sea Aut (G) el grupo de automorfismos de G. La aplicación

$$x \to I_x$$

que asocia a x el automorfismo de G:

$$I_x(g) = x * g * x'$$

es un morfismo sobre

$$I : G \to Int(G)$$

de G en el grupo Int (G) de automorfismos interiores de G. De acuerdo con el teorema enunciado en esta seccion se tendrá un isomorfismo

$$G / H \to Int(G)$$

donde $H = Nu(I)$. Analicemos $H = Nu(I)$.

$$\begin{aligned} x \in Nu(I) &\Leftrightarrow I_x = id_G \\ &\Leftrightarrow x * g * x' = g \text{ cualquiera que sea } g \in G \\ &\Leftrightarrow x * g = g * x \end{aligned}$$

Por lo tanto

$$H = \{x / x * g = g * x, \text{ para todo } g \in G\}$$

Este subgrupo se denomina el centro de G y se lo denota con $\mathfrak{Z}_G$. Por lo tanto

$$\boxed{Int(G) \simeq G/\mathfrak{Z}_G}$$

2. Sea $n \in \mathbf{N}$. Sea W_n el grupo de raíces n-simas de la unidad:

$$\begin{aligned} w_0 &= 1 \\ w_1 &= \cos\frac{2\pi}{n} + i \cdot \operatorname{sen}\frac{2\pi}{n} \\ &\dots \\ w_j &= \cos\frac{2j\pi}{n} + i \cdot \operatorname{sen}\frac{2j\pi}{n} \\ &\dots \\ w_{n-1} &= \cos\frac{2(n-1)\pi}{n} + i \cdot \operatorname{sen}\frac{2(n-1)\pi}{n} \end{aligned}$$

La aplicación $f : \mathbf{Z} \to W_n$ definida por

$$f(m) = \cos\frac{2m\pi}{n} + i \cdot \operatorname{sen}\frac{2m\pi}{n}$$

es, en virtud del Teorema de De Moivre, un morfismo de $(\mathbf{Z}, +, 0)$ en W_n, y es, evidentemente, un morfismo sobre. Determinemos Nu(f).

$$\begin{aligned} k \in Nu(f) &\Leftrightarrow \cos\frac{2k\pi}{n} + i \cdot \operatorname{sen}\frac{2k\pi}{n} = w_0 = 1 \\ &\Leftrightarrow \cos\frac{2k\pi}{n} = 1 \text{ y } \operatorname{sen}\frac{2k\pi}{n} = 0 \\ &\Leftrightarrow \frac{2k\pi}{n} = h \cdot 2\pi = \text{múltiplo de } 2\pi,\ h \in \mathbf{Z} \\ &\Leftrightarrow k \text{ es divisible por } n \\ &\Leftrightarrow k \in (n) = \text{subgrupo de } \mathbf{Z} \text{ de múltiplos de } n. \end{aligned}$$

Por lo tanto se ha demostrado que $Nu(f) = (n)$. En definitiva se tiene el isomorfismo

$$\boxed{\mathbf{Z} / (n) \simeq W_n}$$

3. Sean $\mathbf{R}\# = (\mathbf{R} - \{0\}, \cdot, 1)$ = grupo multiplicativo de números reales no nulos.

$\mathbf{R}^+ = (\mathbf{R}^+, \cdot, 1)$ = grupo multiplicativo de números reales positivos.

$f : \mathbf{R}\# \to \mathbf{R}^+$ la aplicación $f(x) = x^2$.

f es un morfismo y es además un morfismo sobre. En efecto, este hecho nada trivial es consecuencia de la siguiente propiedad de los números reales: todo número real positivo posee una raíz cuadrada en $\mathbf{R}$, o sea dado $r \in \mathbf{R}$, $0 < r$ existe $y \in \mathbf{R}$ tal que $y^2 = r$. Determinemos Nu(f):

$$\begin{aligned} x \in Nu(f) &\Leftrightarrow x^2 = 1 \\ &\Leftrightarrow x = 1 \text{ ó } x = -1 \end{aligned}$$

Por lo tanto se tiene el isomorfismo

$$\boxed{\mathbf{R}\# / \{1, -1\} \simeq \mathbf{R}^+}$$

(Interpretación de este isomorfismo: $\mathbf{R}\# / \{1, -1\}$ consiste de la totalidad de pares $\{x, -x\}$ de números reales $x \neq 0$. El isomorfismo está dado por $\{x, -x\} \to x^2$.)

4. Sea $n \in \mathbf{N}$ tal que $n = p^i \cdot q^j$ donde $i, j \in \mathbf{N}$, p y q son números primos y $p \neq q$.

Sean $\mathbf{Z} / (p^i)$ y $\mathbf{Z} / (q^j)$ los grupos cocientes correspondientes a los subgrupos (p^i) y (q^j) de múltiplos enteros de p^i y q^j, respectivamente. Los elementos de $\mathbf{Z} / (p^i)$ se representan mediante los restos de la división entera por p^i. Si u es uno de estos restos se escribirá $\underline{u}$ para denotar el elemento de $\mathbf{Z} / (p^i)$ asociado. Análogamente con $\mathbf{Z} / (q^j)$.

$$A = \mathbf{Z} / (p^i) \oplus \mathbf{Z} / (q^j)$$

la suma directa de $\mathbf{Z} / (p^i)$ y $\mathbf{Z} / (q^j)$. Un elemento típico de A es de la forma

$$(\underline{u}, \underline{v})$$

donde $u, v \in \mathbf{Z}$ satisfacen

$$0 \leq u < p^i \quad y \quad 0 \leq v < q^j$$

Sean

$$g_p : \mathbf{Z} \to \mathbf{Z} / (p^i) \quad y \quad g_q : \mathbf{Z} \to \mathbf{Z} / (q^j)$$

los morfismos canónicos.

Sea $f : \mathbf{Z} \to A$ la aplicación definida por

$$m \to (g_p(m), g_q(m))$$

f es un morfismo, cuya verificación se deja a cargo del lector.

Afirmación. f es un morfismo sobre. En efecto, siendo p^i y q^j primos entre sí, por suponerse $p \neq q$, existen enteros r, s tales que

$$(:) \qquad rp^i + sq^j = 1$$

(por una propiedad típica del máximo común divisor). Sea entonces $(\underline{u}, \underline{v}) \in A$. El entero

$$m = vrp^i + usq^j$$

satisface

$$f(m) = (g_p(m), g_q(m)) = (g_p(usq^j), g_q(vrp^i))$$

y ahora en virtud de (:) es

$$u = urp^i + usq^j$$
$$v = vrp^i + vsq^j$$

con lo que

$$f(m) = (\underline{u}, \underline{v})$$

lo cual prueba que f es un morfismo sobre.

Calculemos ahora Nu(f).

$$\begin{aligned} m \in Nu(f) &\Leftrightarrow (g_p(m), g_q(m)) = 0 = (\underline{0}, \underline{0}) \\ &\Leftrightarrow p^i \text{ divide a } m \text{ y} \\ &\quad\; q^j \text{ divide a } m \\ &\Leftrightarrow p^i . q^j \text{ divide a } m \end{aligned}$$

(Nota: la última equivalencia es debida a que p^i y q^j son primos entre sí.)

El razonamiento precedente nos muestra entonces que

$$Nu(f) = (p^i . q^j) = (n)$$

= a la totalidad de múltiplos del entero n. Ahora en virtud del teorema de isomorfismo se tiene el isomorfismo fundamental:

$$\mathbf{Z} / (n) \simeq \mathbf{Z} / (p^i) \oplus \mathbf{Z} / (q^j) \quad \text{si} \quad n = p^i . q^j \quad p, q \text{ primos distintos}$$

Como aplicación se tienen los isomorfismos:

a) $\mathbf{Z} / (6) \simeq \mathbf{Z} / (2) \oplus \mathbf{Z} / (3)$
b) $\mathbf{Z} / (12) \simeq \mathbf{Z} / (4) \oplus \mathbf{Z} / (3)$
c) $\mathbf{Z} / (36) \simeq \mathbf{Z} / (4) \oplus \mathbf{Z} / (9)$

Ejercicio. Probar que no existe ningún isomorfismo entre $\mathbf{Z} / (4)$ y $\mathbf{Z} / (2) \oplus \mathbf{Z} / (2)$.

G. Grupos Finitos

Un grupo G se dice finito si G es un conjunto finito, o sea si G es coordinable a un intervalo natural inicial I_k.

$$I_k = \{n / n \in \mathbf{N}, 1 \leq n \leq k\}$$

Se escribe entonces

$$Card(G) = k$$

y se dice también que G es un grupo de orden k.

Históricamente la teoría de grupos finitos está estrechamente ligada a la teoría de la resolución de ecuaciones algebraicas o más generalmente a la llamada Teoría de Galois.

Ejemplo. Sea $n \in \mathbf{N}$ y sea $X = \{1, 2, .., n\}$. Entonces el grupo $G = Tran(X)$ es un grupo de orden $n! =$ factorial de n. Los elementos de Tran(X) se denominan permutaciones. G se denomina el grupo simétrico de grado n y se le denota por $G = S_n$. Este es el ejemplo más importante de grupo finito, dado que: Teorema (Cayley) para todo grupo finito G existe $n \in \mathbf{N}$ y un monomorfismo $G \to S_n$, o sea todo grupo finito es subgrupo de un grupo de permutaciones.

Demostraremos aquí un teorema elemental muy importante, a saber, el Teorema de Lagrange. Previamente será necesario estudiar la cardinalidad de las clases de equivalencia de la relación determinada por un subgrupo. Sea G un grupo y sea H un subgrupo de G. Sea $\sim$ la relación de equivalencia compatible a la izquierda determinada por H, o sea

$$u \sim v \Leftrightarrow v' * u \in H$$

Sea S una clase de equivalencia según $\sim$. Existe entonces $s \in G$ tal que

$$S = \{x / x \sim s\}$$

Afirmación. S y H son conjuntos coordinables. En efecto, sean las aplicaciones

$$f : S \to H \quad \text{definida por} \quad x \to s' * x$$
$$\text{y} \quad g : H \to S \quad \text{definida por} \quad h \to s * h$$

se sigue fácilmente que $g \circ f = id_S$ y $f \circ g = id_H$ de manera que f (y lo mismo g) es una biyección.

Corolario. Dos clases de equivalencia S y T según $\sim$ son coordinables.

En efecto, S es coordinable a H y T es coordinable a H por lo tanto S es coordinable a T.

Teorema. (Lagrange). Sea G un grupo finito. Sea H un subgrupo de G. Entonces si $Card(G/\sim)$ denota el número de elementos del "conjunto" cociente $G/\sim$ (o sea, el número total de clases de equivalencia según $\sim$) se tiene

$$\text{(L)} \qquad Card(G) = Card(H) \cdot Card(G/\sim)$$

Demostración. $\sim$ determina sobre G una partición y los conjuntos de esta partición son todo coordinables entre sí y coordinables a H, según afirma el corolario precedente. Por lo tanto se satisface (L).

77

Corolario. Sea G un grupo finito y sea H un subgrupo de G. Entonces el orden de H divide al orden de G.

Corolario. Sea G un grupo finito y sea H un subgrupo distinguido de G. Entonces

$$Card(G) = Card(H) \cdot Card(G/H)$$

Aplicaciones

1. Todo grupo finito de orden p primo es cíclico, o sea isomorfo a $\mathbf{Z}/(p)$. En efecto, sea G un grupo finito de orden primo p. Entonces si $x \in G$, $x \neq e$ la aplicación $\mathbf{Z} \to G$ definida por

$$f : m \to x^m$$

(donde $x^0 = e$, $x^n = (x^{-n})^{-1}$ si $n < 0$)

es un morfismo tal que

$$Im(f) \neq \{e\}$$

pues $e \neq x \in Im(f)$. Por lo tanto $Im(f)$ es un subgrupo de G de orden mayor que 1 y que (Lagrange) divide a p. Siendo p primo debe ser

$$Im(f) = G$$

Por lo tanto

$$\mathbf{Z} / H \simeq G$$

donde H es el núcleo de f. Puesto que Card $(\mathbf{Z}/H)$ = Card (G) = p debe ser H = (p). Por lo tanto, se tiene finalmente

$$G \simeq \mathbf{Z} / (p)$$

Corolario. Todo grupo finito de orden primo es conmutativo.

2. Todo grupo finito de orden ≤ 5 es conmutativo. En efecto, si Card (G) = 2, 3, 5 entonces es conmutativo según acabamos de ver. Queda entonces por analizar el caso Card (G) = 4. Esto último lo dejamos como ejercicio para el lector. Nótese que hay grupos de orden 6 no conmutativos como, por ejemplo, el grupo simétrico S_3. ¿Es éste el único grupo de orden 6 no conmutativo? Sí.

Ejercicio

i. Construir una tabla de composición del grupo S_3.
ii. Determinar todos sus subgrupos y señalar los distinguidos.
iii. Probar que $\mathfrak{Z}_{S_3} = \{e\}$.
iv. Probar que $Aut(S_3) = Int(S_3)$, o sea que todo automorfismo de S_3 es interior.

Nota. Las siguientes propiedades son válidas en S_n (véase referencia bibliográfica (9)).

s1) Para todo n, $3 \leq n$: $\mathfrak{Z}_{S_n} = \{e\}$.
s2) Para todo n, $3 \leq n$ y $n \neq 6$: $Aut(S_n) = Int(S_n)$.

Ejercicio. Sea p un entero racional primo. Probar que el grupo

$$Aut(Z/(p) \oplus Z/(p))$$

de automorfismos de la suma directa $Z/(p) \oplus Z/(p)$ posee orden $(p^2 - 1) \cdot (p^2 - p)$.

III. ESTRUCTURA DE ANILLO

A. Definición y Ejemplos

No habrá escapado a la atención del lector que ha seguido el tratamiento hecho en el capítulo anterior la posibilidad de introducir en un conjunto más de una ley de composición. Esto efectivamente es posible y da lugar, en particular, a la importante estructura algebraica de anillo. Si • y * son dos leyes de composición definidas sobre un conjunto A, una condición esencial a imponer es que dichas leyes de composición guarden alguna relación entre sí. Una forma natural de establecer relaciones entre ambas es, conforme a los esquemas numéricos, mediante las leyes distributivas. Así diremos que

Definición

* es distributiva a la izquierda respecto de • si

$$x * (y \bullet z) = (x * y) \bullet (x * z)$$

cualesquiera que sean $x, y, z \in A$.

* es distributiva a la derecha respecto de • si

$$(x \bullet y) * z = (x * z) \bullet (y * z)$$

cualesquiera que sean $x, y, z \in A$.

* es distributiva respecto de •, si lo es a la izquierda y a la derecha.

Ciertamente, en el caso que * sea una ley de composición conmutativa los distintos tipos de distributividad antes definidos coinciden entre sí.

Ejemplo. Sea $A = \mathbf{N}$ y sean * y • definidas por

$$a * b = a$$
$$a \bullet b = a + b$$

Es fácil ver entonces que * es distributiva con respecto de • a la derecha, pero no a la izquierda.

Ejemplo. Sea $A = P(X)$ = totalidad de partes de un conjunto X. Sean * y • definidas por $x * y = x \cap y$ $x \bullet y = x \cup y$. En tal caso * es distributiva respecto de • y, recíprocamente, • es distributiva respecto de *.

Suele imponerse otro tipo de condiciones a fin de hacer más sistemático el estudio de estas estructuras con dos leyes de composición. Por ejemplo, se pide que una de ellas sea un semigrupo conmutativo y que la otra ley de composición sea distributiva respecto de la primera. Resulta entonces conveniente introducir la siguiente notación:

+ denotará una ley de composición conmutativa
· denotará una ley de composición genérica

(o sea, a · no le imponemos ninguna condición especial). El caso + se denominará aditivo mientras que el · se denominará multiplicativo. Por abuso de lenguaje llamaremos a + suma y a · producto. Siendo así será conveniente ajustar nuestra notación anterior sobre elementos identidad, inversos, etc., como sigue:

Caso aditivo:	Antes	Ahora
	$*$	$+$
	e	0
	x'	$-x$
Caso multiplicativo:		
	$*$	$\cdot$
	e	1
	x'	x^{-1}

Veamos como se traducen relaciones estudiadas anteriormente:

$$(x * y)' = y' * x' \qquad \begin{cases} -(x+y) = (-y)+(-x) \\ (x \cdot y)^{-1} = y^{-1} \cdot x^{-1} \end{cases}$$

$$(x')' = x \qquad \begin{cases} -(-x) = x \\ (x^{-1})^{-1} = x \end{cases}$$

$$e * e = e \qquad \begin{cases} 0 + 0 = 0 \\ 1 \cdot 1 = 1 \end{cases}$$

Escribimos además en el caso aditivo

$$x - y = x + (-y)$$

Definición. Sean + y · leyes de composición interna definidas sobre un conjunto A. Diremos que las mismas determinan sobre A una estructura de anillo o también que A es (respecto de + y ·) un anillo si existe $0 \in A$ tal que

a1) $(A, +, 0)$ es un grupo conmutativo.
a2) $(A, \cdot\,)$ es un semigrupo.
a3) · es distributiva (o sea a la izquierda y a la derecha) con respecto a +.

Definición. Diremos también que

- A es un anillo conmutativo si $(A, \cdot\,)$ es un semigrupo conmutativo.
- A es un anillo con identidad si existe $1 \in A$ tal que $1 \neq 0$ y $(A, ., 1)$ es un semigrupo con identidad.

En la proposición siguiente se han reunido resultados válidos en todo anillo A. Recuerde el lector que $-x$ denota el inverso aditivo de x y que $x - y$ denota la suma $x + (-y)$.

Proposición. Sea A un anillo, entonces si $a, b, c, d \in A$

i. $a \cdot 0 = 0 \cdot a = 0$
ii. $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$
iii. $(-a) \cdot (-b) = a \cdot b$
iv. $a \cdot (b - c) = a \cdot b - a \cdot c$
v. $(a - b) \cdot c = a \cdot c - b \cdot c$
vi. $(a + b) \cdot (c + d) = a \cdot c + a \cdot d + b \cdot c + b \cdot d$

Demostración. Estará basada en la utilización del teorema de existencia y unicidad de las ecuaciones, sobre el grupo aditivo A, de la forma $a + X = b$.

i. $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ y puesto que también $a \cdot 0 = a \cdot 0 + 0$ se tiene que

$$a \cdot 0 \quad y \quad 0$$

son ambas soluciones de la ecuación $a \cdot 0 + X = a \cdot 0$. Por lo tanto debe ser $a \cdot 0 = 0$. Análogamente, resulta $0 \cdot a = 0$.

ii. $(-a) . b + a \cdot b = ((-a) + a) \cdot b = 0 \cdot b = 0$ y puesto que también $-(a \cdot b) + a \cdot b = 0$ se tiene que

$$(-a) \cdot b \quad y \quad -(a \cdot b)$$

son ambas soluciones de la ecuación $X + a \cdot b = 0$. Por lo tanto debe ser $(-a) \cdot b = -(a \cdot b)$. Análogamente, resulta $a \cdot (-b) = -(a \cdot b)$.

Nota. En virtud de este resultado no hay ambigüedad al escribir $- a \cdot b$ en lugar de $-(a \cdot b)$, ya que asociando el $-$ tanto a a como a $a \cdot b$ no varía la expresión.

iii. $a \cdot b = -(-(a \cdot b))$
$= -((-a) \cdot b)$ en virtud de ii.
$= (-a) \cdot (-b)$ en virtud de ii.

iv. $a \cdot (b - c) = a \cdot (b + (-c)) = a \cdot b + a \cdot (-c)$
$= a \cdot b + (-(a \cdot c)) = a \cdot b - a \cdot c$

v. Demostración análoga a iv.

vi. Se deja a cargo del lector.

Corolario. Sea A un anillo con identidad 1. Entonces las ecuaciones

$$0 \cdot X = 1$$
$$Y \cdot 0 = 1$$

no admiten ninguna solución en A.

Demostración. En efecto, de acuerdo con i $0 \cdot a = a \cdot 0 = 0$ cualquiera que sea $a \in A$. Puesto que además es $1 \neq 0$ (de acuerdo con lo convenido al definir anillo con identidad) ninguna solución en A de cualquiera de esas ecuaciones es posible.

Sea A un anillo con identidad 1. Con

$$U(A)$$

denotamos el subgrupo de (A, ., 1) de elementos inversibles o unidades y lo denominamos el grupo de unidades del anillo A.

Nótese que el corolario anterior es equivalente a la afirmación

$$0 \notin U(A)$$

Definición. Diremos que un anillo con identidad A es un anillo de división si

$$U(A) = A - \{0\}$$

o sea si todo elemento $a \in A$ con $a \neq 0$ es inversible en (A, ., 1).

Definición. Llamaremos cuerpo (se suele utilizar también la denominación campo) a todo anillo de división conmutativo.

Ejemplos

1. Anillos numéricos

   i. **Z** con + = suma ordinaria y · = producto ordinario es un anillo conmutativo con identidad: el anillo de enteros racionales. $U(\mathbf{Z}) = \{1, -1\}$.

   ii. **Q** con + = suma ordinaria y · = producto ordinario es un anillo conmutativo con elemento identidad. $U(\mathbf{Q}) = \mathbf{Q}^{\#} = \mathbf{Q} - \{0\}$. **Q** es el cuerpo de los números racionales.

En forma análoga a ii

   iii. **R** es el cuerpo de los números reales.

   iv. **C** es el cuerpo de los números complejos.

2. Sea A = (A, +, 0) un grupo conmutativo. Sea (A, .) la estructura de semigrupo trivial:

$$x \cdot y = 0$$

cualesquiera que sean $x, y \in A$. Entonces + y · definen sobre A una estructura de anillo conmutativo: el anillo trivial asociado al grupo conmutativo A.

3. Sea X un conjunto y sea $A = \mathcal{P}(X)$ el conjunto de partes de X. Las dos siguientes leyes de composición sobre A:

$$x + y = x \Delta y = \text{diferencia simétrica de } x \text{ e } y$$
$$x \cdot y = x \cap y = \text{intersección de } x \text{ e } y$$

determinan sobre A una estructura de anillo conmutativo con identidad: el anillo de Boole de subconjuntos de X. Se verifica $U(A) = \{X\}$, o sea el único elemento inversible de A es la identidad $1 = X$.

4. Sea M = (M, +, 0) un grupo conmutativo. Sea End(M) = (End(M), o) el semigrupo de endomorfismos de M. Vamos a definir sobre End(M) la siguiente "suma". Sean $f, g \in End(M)$.

Entonces si $m \in M$:

(.) $$m \rightarrow f(m) + g(m)$$

define una aplicación de M en M que satisface

(:) $$\begin{aligned} m_1 + m_2 \rightarrow f(m_1 + m_2) + g(m_1 + m_2) &= \\ f(m_1)+f(m_2) + g(m_1) + g(m_2) &= \\ [f(m_1) + g(m_1)] + [f(m_2) + g(m_2)] \end{aligned}$$

(Nótese que en el último paso se ha hecho uso de la conmutatividad de M al permutar $f(m_2)$ con $g(m_1)$.) (:) muestra entonces que la aplicación (.) es un morfismo de M, o sea un elemento de End(M). Este nuevo morfismo se denotará con $f + g$. En símbolos

(·) $$\boxed{(f + g)(m) = f(m) + g(m) \quad \text{si} \quad m \in M}$$

Por lo tanto

$$(f, g) \rightarrow f + g$$

define una ley de composición en End(M), o sea una estructura de monoide (End(M), +), que satisface

a) $f + g = g + f$. En efecto,

$$\begin{aligned} (f + g)(m) &= f(m) + g(m) \\ &= g(m) + f(m) \end{aligned} \Big\} \text{ conmutatividad de M}$$
$$= (g + f)(m), \text{ si } m \in M$$

lo que confirma nuestra afirmación.

b) $f + (g + h) = (f + g) + h$, si $f, g, h \in \text{End}(M)$. En efecto, basta aplicar la definición (·) y utilizar la propiedad asociativa de (M, +, 0).

c) La aplicación denotada por $\underline{0} : M \rightarrow M$ definida por

$$\underline{0}(m) = 0, \quad \text{si} \quad m \in M$$

satisface

$$\underline{0} + f = f + \underline{0} = f$$

de manera que $\underline{0}$ es elemento identidad de (End (M), +).

d) Sea $f \in \text{End}(M)$. La aplicación $f' : \rightarrow M$ definida por

$$f'(m) = -f(m) \quad \text{si} \quad m \in M$$

es un morfismo:

$$\begin{aligned} f'(m_1 + m_2) &= -f(m_1 + m_2) = -(f(m_1) + f(m_2)) \\ &= -f(m_1) + (-f(m_2)) \\ &= f'(m_1) + f'(m_2) \end{aligned}$$

Satisface además

$$(f + f')(m) = f(m) + f'(m) = f(m) + (-f(m)) = 0 = \underline{0}(m)$$

o sea

$$f + f' = \underline{0}$$

Pero por a) sigue que

$$f' + f = \underline{0}$$

Por lo tanto f' es inverso de f en (End(M), +, $\underline{0}$).

En definitiva, la ley de composición f + g definida en End(M) es una ley de composición de grupo conmutativo.

Afirmamos ahora que las leyes de composición en End(M) f + g y f o g definen una estructura de anillo.

En efecto, habrá que probar las leyes distributivas

$$f \circ (g + h) = f \circ g + f \circ h$$
$$(f + g) \circ h = f \circ g + g \circ h$$

La demostración es similar en ambos casos, probemos la primera:

$$\begin{aligned}[f \circ (g + h)](m) &= f((g + h)(m)) \\ &= f(g(m) + h(m)) \\ &= f(g(m)) + f(h(m)) \\ &= (f \circ g)(m) + (f \circ h)(m), \\ &\quad \text{si } m \in M\end{aligned}$$

Por lo tanto la distributividad pedida.

El anillo así definido es de extrema importancia en álgebra y se le denomina el anillo de endomorfismos de (el grupo conmutativo) M. Es un anillo con identidad, dado que (End(M), o) es un semigrupo con identidad. En general, no es un anillo conmutativo. Demostremos esta última afirmación con un ejemplo sencillo. Sea **Z**/(2) = {0, 1} = el grupo de restos módulo 2. La estructura de grupo conmutativo de **Z**/(2) está dada por 0 + 0 = 0, 1 + 0 = 0 + 1 = 1, 1 + 1 = 0. Sea M = **Z**/(2) ⊕ **Z**/(2) = suma directa de **Z**/(2) consigo mismo. La descripción de M es la siguiente:

$$M = \{(0,0), (0,1), (1,0), (1,1)\}$$

+	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 0)	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 1)	(0, 1)	(0, 0)	(1, 1)	(1, 0)
(1, 0)	(1, 0)	(1, 1)	(0, 0)	(0, 1)
(1, 1)	(1, 1)	(1, 0)	(0, 1)	(0, 0)

(0, 0) es la identidad de (M, +). Sean f, g aplicaciones de M en M definidas por

$$f: \begin{array}{l}(0,0) \to (0,0) \\ (1,0) \to (1,0) \\ (0,1) \to (1,0) \\ (1,1) \to (0,0)\end{array} \qquad g: \begin{array}{l}(0,0) \to (0,0) \\ (1,0) \to (1,1) \\ (0,1) \to (0,0) \\ (1,1) \to (1,1)\end{array}$$

Se deja al lector el verificar que f y g son endomorfismos de M. Probemos que f o g ≠ g o f. En efecto,

$$(f \circ g)\,(1,0) = (0,0)$$
$$(g \circ f)\,(1,0) = (1,1)$$

lo cual comprueba nuestra afirmación. Consecuentemente, End(M) no es un anillo conmutativo. Otra característica de este ejemplo es que $f \neq \underline{0}$, $g \neq \underline{0}$ y sin embargo

$$f \circ g = \underline{0}$$
$$\text{y} \qquad g \circ f \neq \underline{0}$$

5. Sea S un anillo y sea X un conjunto no vacío. Sea A = Aplc(X, S) la totalidad de aplicaciones de X en S. Las leyes de composición + y $\cdot$ en S dan lugar, según se vió oportunamente, a leyes de composición en Aplc(X, S):

$$f + g : x \to f(x) + g(x)$$
$$f \cdot g : x \to f(x) \cdot g(x)$$

que denominamos las leyes de composición puntual de f con g respecto de + y $\cdot$, respectivamente. Además, si $\underline{0} \in A$ denota la aplicación constante

$$\underline{0}(x) = 0, \text{ si } x \in X$$

se tiene que $(A, +, \underline{0})$ es un grupo conmutativo. Por otra parte, (A, .) es un semigrupo. Es fácil verificar la distributividad de $\cdot$ respecto de +, de manera que queda definido sobre A una estructura de anillo: el <u>anillo de aplicaciones (o funciones) de X en S</u>. Es un anillo conmutativo si S lo es y posee identidad si S lo posee. (Este ejemplo es de gran importancia en análisis y, en especial, en la situación siguiente: $X = \mathbf{R}^n$ el espacio euclidiano n-dimensional y S = el cuerpo **R** de los números reales y donde las aplicaciones se restringen a las "aplicaciones continuas".)

6. En el ejemplo 2 se ha demostrado cómo introducir una estructura de anillo en un grupo conmutativo A. En general, se puede formular el siguiente problema: dado un grupo conmutativo A, ¿cuántas estructuras posibles de anillo se pueden definir sobre A que conserven la estructura de grupo conmutativo original? Por ejemplo, el lector puede probar, a manera de ejercicio, que la única estructura de anillo <u>con identidad</u> que puede definirse sobre (**Z**, +, 0) es la estructura ordinaria. Lo mismo es cierto para los grupos cocientes **Z**/(m). Es interesante el siguiente resultado: la única estructura de anillo definible sobre el grupo cociente **Q**/**Z**, es la trivial, o sea $x \cdot y = 0$ cualesquiera que sean $x, y \in$ **Q**/**Z**. La demostración es muy sencilla. El análisis de un caso particular sugerirá al lector la demostración general. Supongamos pues definida sobre **Q**/**Z** una estructura de anillo. Entonces (por ejemplo):

$$\begin{aligned}[1/2]\cdot[1/3] &= [3\cdot 1/6]\cdot[1/3]\\ &= [1/6]\cdot[1/3] + [1/6]\cdot[1/3] + [1/6]\cdot[1/3]\\ &= [1/6]\cdot([1/3] + [1/3] + [1/3])\\ &= [1/6]\cdot[1]\\ &= [1/6]\cdot 0\\ &= 0\end{aligned}$$

7. Sean

A = anillo

$n \in \mathbf{N}$

I_n = intervalo natural inicial = $\{k/k \in \mathbf{N}$ y $1 \le k \le n\}$.

Formemos el producto cartesiano $J = I_n \times I_n$. Anteriormente habíamos estudiado el semigrupo $(\mathrm{Apl}(J, A), +)$ de aplicaciones de J en el grupo conmutativo $(A, +, 0)$. Recordemos que si $f, g \in \mathrm{Apl}(J, A)$ entonces

(') $$(f + g)(x) = f(x) + g(x)$$

En nuestro caso $x \in J$ es de la forma $x = (i, j)$. Convendremos en escribir

$$f(i, j) = f_{ij} \quad \text{si} \quad f \in \mathrm{Apl}(J, A)$$

(') se escribe entonces

$$\boxed{(f + g)_{ij} = f_{ij} + g_{ij}}$$

Definimos ahora sobre $\mathrm{Apl}(J, A)$ un producto: $(f, g) \to f \cdot g$ por

$$\boxed{\begin{aligned}(f\cdot g)_{ij} &= \sum_{k=1}^{n} f_{ik}\cdot g_{kj}\\ &= f_{i1}\cdot g_{1j} + f_{i2}\cdot g_{2j} + \dots + f_{in}\cdot g_{nj}\end{aligned}}$$

Un cálculo sencillo nos muestra que $(\mathrm{Apl}(J, A), .)$ es un semigrupo y además que $\cdot$ distribuye respecto de $+$. O sea $+$ y $\cdot$ definen sobre $\mathrm{Apl}(J, A)$ una estructura de anillo. Es útil representar los elementos de $\mathrm{Apl}(J, A)$ mediante "cuadros" denominados <u>matrices de n filas por n columnas</u>

$$f \leftrightarrow \begin{Vmatrix} f_{11} & f_{12} & \cdots & f_{1n}\\ f_{21} & f_{22} & \cdots & f_{2n}\\ \cdot & \cdot & \cdots & \cdot\\ \cdot & \cdot & \cdots & \cdot\\ f_{n1} & f_{n2} & \cdots & f_{nn}\end{Vmatrix}$$

La suma y el producto se expresan entonces, en el caso $n = 2$,

$$\begin{Vmatrix} f_{11} & f_{12}\\ f_{21} & f_{22}\end{Vmatrix} + \begin{Vmatrix} g_{11} & g_{12}\\ g_{21} & g_{22}\end{Vmatrix} = \begin{Vmatrix} f_{11} + g_{11} & f_{12} + g_{12}\\ f_{21} + g_{21} & f_{22} \quad g_{22}\end{Vmatrix}$$

$$\begin{Vmatrix} f_{11} & f_{12}\\ f_{21} & f_{22}\end{Vmatrix} \quad \begin{Vmatrix} g_{11} & g_{12}\\ g_{21} & g_{22}\end{Vmatrix} = \begin{Vmatrix} f_{11}\cdot g_{11} + f_{12}\cdot g_{21} & f_{11}\cdot g_{12} + f_{12}\cdot g_{22}\\ f_{21}\cdot g_{11} + f_{22}\cdot g_{21} & f_{21}\cdot g_{12} + f_{22}\cdot g_{22}\end{Vmatrix}$$

El anillo así obtenido se denomina anillo completo de matrices con coeficientes en A de n filas por n columnas (o, brevemente, el anillo de matrices de $n \times n$ sobre A). Se le denota por $M_n(A)$. Veamos algunas propiedades de $M_n(A)$:

a) Si A posee elemento identidad 1 entonces $M_n(A)$ posee elemento identidad. En efecto, la matriz

$$e = \begin{Vmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & 1 \end{Vmatrix} \qquad \text{o sea} \quad e_{ij} = \begin{cases} 0 & \text{si} \quad i \neq j \\ 1 & \text{si} \quad i = j \end{cases}$$

es identidad de $M_n(A)$.

b) Sea A un anillo con identidad. Entonces si $1 < n$, $M_n(A)$ no es un anillo conmutativo. En efecto, veamos el caso $n = 2$

$$\begin{Vmatrix} 0 & 1 \\ 0 & 0 \end{Vmatrix} \cdot \begin{Vmatrix} 1 & 0 \\ 0 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & 0 \\ 0 & 0 \end{Vmatrix} = 0$$

$$\begin{Vmatrix} 1 & 0 \\ 0 & 0 \end{Vmatrix} \cdot \begin{Vmatrix} 0 & 1 \\ 0 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & 1 \\ 0 & 0 \end{Vmatrix} \neq 0$$

c) Sea A un anillo con identidad. Entonces, si $1 < n$, existen elementos $x, y \in M_n(A)$ tales que

$$x \neq 0, \; y \neq 0 \quad \text{y} \quad x \cdot y = 0$$

(El ejemplo anterior demuestra ese hecho.)

Es interesante y también importante analizar el semigrupo multiplicativo de $M_n(A)$, suponiendo a A un anillo con identidad. El grupo $U(M_n(A))$ de elementos inversibles de $M_n(A)$ recibe entonces el nombre de grupo lineal general de grado n con coeficientes en A y se le denota por $GL_n(A)$. Los grupos más importantes de la geometría son grupos de este tipo, A es generalmente un cuerpo. Para las aplicaciones aritméticas A es un anillo conmutativo. El interés de estudiar $M_n(A)$ en el caso de un anillo conmutativo con identidad radica en la existencia de la Teoría de Determinantes. Sin entrar a detallar esta teoría digamos brevemente que en la misma se demuestra la existencia de una aplicación

$$\text{Det} : M_n(A) \rightarrow A$$

entre cuyas propiedades está la de ser un morfismo de las estructuras multiplicativas, o sea

$$\begin{aligned} \text{Det}(f \cdot g) &= \text{Det}(f) \cdot \text{Det}(g) \\ \text{Det}(e) &= 1 \end{aligned}$$

donde e denota el elemento identidad de $M_n(A)$.

En términos de la teoría de determinantes es posible formular el siguiente criterio de caracterización de $GL_n(A)$, sea $f \in M_n(A)$

$$f \in GL_n(A) \quad \text{si, y sólo si,} \quad Det(f) \in U(A)$$

En el caso particular de ser A un cuerpo, siendo $U(A) = A - \{0\}$, se tiene

$$f \in GL_n(A) \quad \text{si, y sólo si,} \quad Det(f) \neq 0$$

(El ser determinante un morfismo da una demostración de la parte "sólo si" del criterio.)

B. Subanillos e Ideales

En esta sección se estudiarán las subestructuras características de un anillo.

Sea A un anillo y C un subconjunto de A.

Definición. Diremos que C es un subanillo de A si

s1) C es subgrupo de $(A, +, 0)$.
s2) C es subsemigrupo de $(A, .)$.

El lector puede verificar, a manera de ejercicio, la validez de la siguiente proposición.

Proposición. Un subconjunto C de un anillo A es un subanillo si, y sólo si, satisface todas las propiedades siguientes:

1. $C \neq \emptyset$
2. $x \in C, y \in C \rightarrow x - y \in C$
3. $x \in C, y \in C \rightarrow x\, y \in C$

Ejemplos

1. Para todo anillo A, $C = \{0\}$ y $C = A$ son subanillos de A.

2. Sea A un anillo trivial. Entonces todo subgrupo C de A es un subanillo.

3. Sea **Z** el anillo de enteros racionales. Entonces todo subgrupo de $(\mathbf{Z}, +, 0)$ es un subanillo. En efecto, si C es subgrupo de **Z** existe $m \in Z$, tal que $C = (m)$ = la totalidad de múltiplos enteros de m. Como el producto de dos múltiplos de m es también un múltiplo de m se sigue que la condición 3 de la proposición se satisface y C es entonces un subanillo de **Z**. Note el lector la verificación en **Z** de la siguiente propiedad más fuerte que la condición 3.

$$3'.\ n \in Z \ \text{ y } \ r \in C \Rightarrow n \cdot r \in C$$

4. Sea X un conjunto y sea $A = Aplc(X, S)$ = el anillo de aplicaciones de X en un anillo S. Sea Y un subconjunto no vacío de X. Entonces

$$C = \{f / f \in \text{Aplc}(X,S) \quad \text{con} \quad f(y) = 0 \quad \text{si } y \in Y\}$$

es un subanillo de A : el subanillo de aplicaciones nulas sobre Y. En efecto, utilizando la proposición 3, sean f, g $\in$ Aplc (X, S).

1) $\underline{0} \in C$.

2) Si f, g $\in$ C e y $\in$ Y se tiene $(f - g)(y) = f(y) - g(y) = 0 - 0 = 0$. Por lo tanto $f - g \in C$.

3) Si f, g $\in$ C e y $\in$ Y se tiene $(f \cdot g)(y) = f(y) \cdot g(y) = 0 \cdot 0 = 0$.

Por lo tanto, C es subanillo de A. Nótese también aquí que en lugar de 3 se verifica la condición más fuerte

$$3'. \quad f \in A \ \text{ y } \ g \in C \Rightarrow f \cdot g \in C$$

5. Sea p un número primo. Sea $\mathbf{Q}$ el cuerpo de los números racionales. Sea $C \subset \mathbf{Q}$ definido por:

$y \in C$ si, y sólo si, existen $r, s \in \mathbf{Z}$ tales que $(p, s) = 1$ e $y = r/s$

Notemos que $1 \in C$. El lector puede comprobar fácilmente la verificación de 2 y 3 de la proposición. C es pues un subanillo de $\mathbf{Q}$ que se suele denotar por $\mathbf{Z}_{(p)}$ y se le denomina localización de $\mathbf{Z}$ en el primo p. $\mathbf{Z}_{(p)}$ es de suma importancia en la Teoría Algebraica de Números.

6. Un ejemplo finito. Sea A el anillo definido por las tablas

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	2	0	2
2	0	0	0	0
3	0	2	0	2

Entonces los subanillos de A son

$$C = \{0\}, \ C = \{0, 2\}, \ C = A$$

Numerosas situaciones (como en los ejemplos 3 y 4) y el desarrollo posterior de la teoría sugieren ampliar la definición de subanillo, cambiando la condición 3 en la proposición.

Definición. Diremos que un subconjunto C de un anillo A es

i. Un ideal a la izquierda de A si satisface 1 y 2 de la proposición y además la condición

$$3'. \quad x \in A \ \text{ y } \ c \in C \Rightarrow x \cdot c \in C$$

ii. Un ideal a la derecha de A si satisface 1 y 2 de la proposición y además la condición

$$3''. \quad c \in C \ \text{ y } \ x \in A \Rightarrow c \cdot x \in C$$

iii. Un ideal bilátero de A, si es ideal a la izquierda y a la derecha de A.

Por cierto que en el caso de un anillo conmutativo no es necesario hacer distinción entre estos conceptos y se puede hablar simplemente de ideales. Se suele también utilizar la palabra ideal como sinónimo de ideal bilátero. Antes de entrar en ejemplos se da el siguiente ejercicio.

Ejercicio. Sea A un anillo con identidad. Sea J un ideal a la izquierda (o a la derecha) de A. Entonces si $J \neq A$ es

$$J \cap U(A) = \phi$$

En particular si $1 \in J$ se tiene $J = A$.

Ejemplos

1. Para todo anillo A, $C = \{0\}$ y $C = A$ son ideales biláteros de A.

2. Sea A un anillo trivial. Entonces todo subgrupo de $(A, +, 0)$ es un ideal bilátero de A.

3. En el anillo **Z** de enteros racionales los siguientes conceptos coinciden: subgrupo de $(\mathbf{Z}, +, 0)$, subanillo, ideal bilátero.

4. Sea $A = \mathrm{Aplc}(X, S)$ el anillo de aplicaciones de X en un anillo S. Sea Y un subconjunto no vacío de X. Entonces el subanillo de aplicaciones nulas sobre Y es un ideal bilátero de A.

5. Sea $\mathbf{Z}_{(p)}$ la localización de **Z** en el primo p, o sea la totalidad de números racionales que pueden expresarse por fracciones con denominador no divisible por p. Sea $I \subset \mathbf{Z}_{(p)}$ la totalidad de dichas fracciones cuyo numerador es divisible por p. Entonces I es un ideal bilátero de $\mathbf{Z}_{(p)}$. Es fácil ver que $U(\mathbf{Z}_{(p)})$ = grupo de unidades de $Z_{(p)} = Z_{(p)} - I$ = complemento de I en $Z_{(p)}$. Como consecuencia se tiene que todo ideal J de $Z_{(p)}$ tal que $J \neq Z_{(p)}$ está contenido en I. Anillos con esta propiedad se denominan anillos locales por razones derivadas de la geometría algebraica.

6. Sea A un anillo y sea $a \in A$. Entonces la totalidad J de elementos de A que son "múltiplos a la izquierda de a" forman un ideal a la izquierda de A. O sea, $y \in J$ si, y sólo si, existe $z \in A$ tal que $y = z \cdot a$ y la verificación que J es ideal a la izquierda es inmediata. Se suele utilizar la notación $J = A \cdot a$ para denotar este ideal.

7. Sea A un anillo y sea U un subconjunto no vacío. Sea J la totalidad de elementos z que satisfacen

$$z \cdot u = 0 \quad \text{para todo} \quad u \in U$$

Entonces J es un ideal a la izquierda de A y se le denomina el anulador a la izquierda de U. En particular, si U consta de un solo elemento a, se denomina J el anulador a la izquierda. Por ejemplo, en Z

N. B. "Ideal bilátero" se utiliza exclusivamente en la Argentina; en otros países se dice también "ideal bilateral".

$$J = 0 \text{ si } U \neq \{0\}$$
$$J = Z \text{ si } U = \{0\}$$

8. En un anillo de división A, $J = \{0\}$ y $J = A$ son los únicos ideales a la izquierda de A. En efecto, sea $J \neq 0$ un ideal a la izquierda y sea $u \in J$ con $u \neq 0$. Entonces por ser A un anillo de división, u es inversible en A o sea existe u^{-1}. Por lo tanto, por la definición de ideal a la izquierda

$$1 = u^{-1} \cdot u \in J$$

Pero, entonces, si $a \in A$

$$a = a \cdot 1 \in J$$

o sea $A \subset J$, luego $A = J$.

Es ejercicio interesante el probar una afirmación recíproca de la anterior, o sea: si A es un anillo cuyos únicos ideales a la izquierda son $\{0\}$ y A, entonces A es un anillo trivial o A es un anillo de división (véase ejemplos 6 y 7).*

Ejercicio. Sea A un anillo de división. Sean $x, z \in A$. Probar que $x \cdot z = 0$ si, y sólo si, $x = 0$ o $z = 0$.

C. Morfismos de Anillos

Sean A y B anillos. Sea $f : A \to B$ una aplicación de A en B.

Definición. Diremos que f es un morfismo de las estructuras de anillo, o simplemente que es un morfismo, si

$$f : (A, +) \to (B, +)$$
$$f : (A, \cdot) \to (B, \cdot)$$

son morfismos de los monoides correspondientes. Explícitamente dicho, si cualesquiera que sean $x, y \in A$

$$f(x + y) = f(x) + f(y)$$
$$f(x \cdot y) = f(x) \cdot f(x)$$

y, además, si A y B poseen elementos identidad $f(1) = 1$.

Los conceptos de monomorfismo, morfismo sobre, isomorfismo, endomorfismo, automorfismo corresponden a las estructuras de monoide.

Ejemplos

0. Sea A un anillo. Entonces la aplicación identidad id_A es un automorfismo de (la estructura de anillo de) A.

1. Sean A y B anillos y sea A un anillo de división. Entonces, si $f : A \to B$ es un morfismo, caben dos únicas posibilidades:

* Un célebre teorema enunciado y probado por J. H. M. Wedderburn, en 1905, establece que todo anillo de división finito es conmutativo. Resulta, pues, infructuoso tratar de encontrar ejemplos de anillos de división no conmutativos finitos. El ejemplo más sencillo de anillo de división, no conmutativo, es el anillo de los cuaterniones descubierto hace más de 100 años por W. R. Hamilton (Referencia (7)).

i. f es el morfismo trivial: $f(x) = 0$ cualquiera que sea $x \in A$, o
ii. f es un monomorfismo.

En efecto, si el caso i no ocurre, existe $x \in A$ tal que $0 \neq y = f(x)$. Para probar que f es un monomorfismo es suficiente, según vimos antes, probar que $Nu(f) = 0$. Sea pues $0 \neq a \in A$. Siendo A un anillo de división existe $a^{-1} \in A$. Entonces

$$0 \neq y = f(x) = f(x \cdot a^{-1} \cdot a) = f(x \cdot a^{-1}) \cdot f(a)$$

lo cual implica $f(a) \neq 0$. Hemos probado pues que $a \neq 0 \Rightarrow f(a) \neq 0$. Equivalentemente, $f(a) = 0 \Rightarrow a = 0$ o sea $Nu(f) = 0$.

2. Sea $\mathbf{Z}$ el anillo de enteros racionales. Sea $f: \mathbf{Z} \to \mathbf{Z}$ un endomorfismo (de la estructura de anillo). Puesto que $f(1) = 1$, se tiene que $f(n) = n$ cualquiera que sea $n \in \mathbf{Z}$ $n \geq 0$. Siendo $f(-m) = -f(m)$, se tiene que $f(m) = m$ cualquiera que sea $m \in \mathbf{Z}$, o sea $f = id_{\mathbf{Z}}$. Se deja al lector verificar que si $A = \mathbf{Q}$ el cuerpo de los números racionales vale también, y que $id_{\mathbf{Q}}$ es el único endomorfismo (de la estructura de anillo de) $\mathbf{Q}$.

3. Sea $\mathbf{R}$ el cuerpo de los números reales. Sea $f: \mathbf{R} \to \mathbf{R}$ un endomorfismo de (la estructura de anillo de) $\mathbf{R}$. Entonces, puesto que $f(1) = 1$, se tiene (según 2) que $f(m) = m$ si $m \in \mathbf{Z}$ y, más aún, utilizando la segunda parte de 2,

$$f(q) = q \quad \text{si} \quad q \in \mathbf{Q}$$

Sea $x \in R$, $0 < x$. Existe entonces $y \in \mathbf{R}$ tal que $y^2 = x$. Por lo tanto

$$f(x) = f(y^2) = f(y) \cdot f(y) = f(y)^2$$

de manera que $f(x) \geq 0$. La situación $f(x) = 0$ debe excluirse en virtud de lo expuesto en el ejemplo 1. Se ha probado pues que

$$0 < x \Rightarrow 0 < f(x)$$

Sea ahora $0 < x$. Si $f(x) \neq x$ cabe entonces las dos posibilidades siguientes

i. $0 < f(x) < x$
ii. $0 < x < f(x)$

En la situacion i, sea $q \in \mathbf{Q}$ tal que $f(x) < q < x$. Entonces $0 < x - q$ de manera que

$$0 < f(x - q) = f(x) - f(q) = f(x) - q$$

lo cual implica

$$q < f(x)$$

en contra de la elección de q. Esta situación no es pues posible.

En la situación ii, sea $q \in \mathbf{Q}$ tal que $x < q < f(x)$. Entonces

de manera que

$$0 < q - x$$

$$0 < f(q - x) = f(q) - f(x) = q - f(x)$$

lo cual implica

$$f(x) < q$$

que contradice la elección de q. Esta situación tampoco es posible.

En definitiva, se ha probado que si $x \in \mathbf{R}$ satisface $0 \leq x$, entonces $f(x) = x$. Ahora como $f(-x) = -f(x)$ se tiene el importante resultado : $id_{\mathbf{R}}$ es el único endomorfismo de (la estructura de anillo de) **R**. (Nótese que en esta demostración se han utilizado propiedades finas de **R**, como son la existencia de raíces cuadradas de números positivos y la llamada "densidad" de **Q** en **R**, que afirma que dados dos números reales a y b, $a < b$ existe siempre un número racional q que satisface $a < q < b$.)

Ejercicio. Sea A un anillo con identidad y sean k, r enteros positivos. Probar que si k/r existe, entonces un monomorfismo $M_k(A) \to M_r(A)$.

D. Relaciones de Equivalencia Compatibles

Analizaremos la compatibilidad de una relación de equivalencia $\sim$ definida sobre un anillo A, con respecto a la estructura de anillo.

Definición. Diremos que $\sim$ es compatible a la izquierda (con la estructura de anillo de A) si

$$a \in A \quad y \quad u \sim v \Rightarrow \begin{cases} a + u \sim a + v \\ a \cdot u \sim a \cdot v \end{cases}$$

Diremos que $\sim$ es compatible a la derecha (con la estructura de anillo de A) si

$$c \in A \quad y \quad u \sim v \Rightarrow \begin{cases} c + u \sim c + v \\ u \cdot c \sim v \cdot c \end{cases}$$

Diremos que $\sim$ es compatible (con la estructura de anillo de A) si es compatible a la izquierda y a la derecha.

Las características de las relaciones de equivalencia compatibles a la izquierda están dadas por el siguiente teorema. •

Teorema. Sea A un anillo. Entonces

1) Si $\sim$ es una relación de equivalencia compatible a la izquierda, el subconjunto I de A definido por

$$I = \{a / a \sim 0\}$$

es un ideal a la izquierda de A que satisface

$$a \sim b \Leftrightarrow a - b \in I$$

Recíprocamente

2) Si I es un ideal a la izquierda de A entonces la relación

(-) $$a \sim b \Leftrightarrow a - b \in I$$

es una relación de equivalencia sobre A compatible a la izquierda.

Demostración

1. Restringida $\sim$ a la estructura aditiva de A resulta, en virtud del teorema análogo demostrado para grupos, que I es un subgrupo de $(A, +, 0)$ y, además, que $a \sim b$ es equivalente a $a - b \in I$. Vamos a demostrar que I es ideal a la izquierda. Sea $a \in A$ y sea $x \in I$. Entonces $x \sim 0$ y por lo tanto $a \cdot x \sim a \cdot 0$, o sea $a \cdot x \sim 0$ de manera que $a \cdot x \in I$.

2. Según el teorema citado en la parte 1 de la demostración, (-) es una relación de equivalencia compatible con $(A, +, 0)$. Vamos a demostrar que es compatible a la izquierda con respecto a $(A, .)$. Sea $a \sim b$ y sea $x \in A$. Entonces $a - b \in I$ y por lo tanto

$$x \cdot a - x \cdot b = x \cdot (a - b) \in I$$

con lo que

$$x \cdot a \sim x \cdot b$$

conforme queríamos probar.

En forma análoga al desarrollo seguido para grupos se llega al resultado importante que establece una biyección entre la clase de relaciones de equivalencia compatibles a la izquierda con la estructura de anillo en A y la clase de ideales a la izquierda de A. Idéntico resultado vale para las relaciones de equivalencia compatibles a la derecha e ideales a la derecha de A.

El resultado obtenido al estudiar las relaciones de equivalencia en grupos que caracterizaban a los subgrupos distinguidos tiene el siguiente análogo:

Teorema. Sea una relación de equivalencia definida sobre un anillo A. Entonces $\sim$ es compatible con la estructura de anillo de A si, y sólo si, el ideal a la izquierda asociado a $\sim$ es bilátero.

Demostración. Sea $\sim$ compatible. Entonces el ideal a la izquierda

$$I = \{a / a \sim 0\}$$

asociado a $\sim$ es bilátero. En efecto, si $a \in I$ entonces

$$a \sim 0$$

y por la compatibilidad a la derecha de $\sim$, se tiene que si $x \in A$

$$a \cdot x \sim 0 \cdot x = 0$$

lo cual implica

$$a \cdot x \in I$$

con lo que queda demostrada nuestra afirmación.

Recíprocamente, sea $I = \{a / a \sim 0\}$ un ideal bilátero. Entonces si $a \sim b$ y $x \in A$ se tiene

$$a - b \in I \quad y \quad (a - b) \cdot x \in I$$

por lo tanto

$$a \cdot x - b \cdot x \in I$$

que equivale a

$$a \cdot x \sim b \cdot x$$

Puesto que por el teorema anterior $\sim$ es compatible a la izquierda el teorema queda probado.

Ha quedado pues establecida una biyección entre la clase de relaciones de equivalencia definidas sobre un anillo A y compatibles con la estructura de anillo y la clase de ideales biláteros de A.

Es posible ahora, de modo similar a lo efectuado al estudiar grupos, plantearnos el problema de definir una estructura de anillo en el conjunto cociente $A / \sim$ de un anillo A por una relación de equivalencia compatible $\sim$, que convierta a la aplicación canónica

$$\varphi : A \rightarrow A / \sim$$

en un morfismo de anillo. Entonces:

Teorema. Sea A un anillo y sea $\sim$ una relación de equivalencia definida sobre A y compatible (a la izquierda y a la derecha) con la estructura de anillo de A.

Sea $A / \sim$ el conjunto cociente de A por $\sim$ y sea $\varphi : A \rightarrow A / \sim$ la aplicación canónica. Entonces

1) Existe una UNICA estructura de anillo sobre $A / \sim$ que convierte a φ en un morfismo de anillos.

2) $Nu(\varphi)$ = el ideal bilátero asociado a $\sim$.

Demostración

1. Por los resultados correspondientes a grupo cociente sabemos que sobre $A / \sim$ está definida una ley de composición de grupo conmutativo

$$(A / \sim, +, 0)$$

que convierte a $\varphi : A \rightarrow A / \sim$ en un morfismo de grupos

$$(A, +, 0) \rightarrow (A / \sim, +, 0)$$

Queda entonces por definir una estructura de semigrupo sobre $A / \sim$ distributiva respecto de +. La definición es análoga. Sea S y T $\in A/\sim$. Existen entonces s y t $\in$ G tales que

$$S = \{x / x \sim s\} = \varphi(s)$$
$$T = \{x / x \sim t\} = \varphi(t)$$

Es fácil ver que el elemento

$$\mathcal{g}(s \cdot t)$$

está unívocamente determinado por S y T, de manera que

$$\begin{cases}(S, T) \rightarrow \mathcal{g}(s \cdot t) \\ \text{si} \quad s \in S \text{ y } t \in T\end{cases}$$

define sobre $A/\sim$ una ley de composición, que denotamos también por

$$(S, T) \rightarrow S \cdot T$$

Se tiene además

$$\mathcal{g}(s \cdot t) = S \cdot T = \mathcal{g}(s) \cdot \mathcal{g}(t)$$

de manera que $\mathcal{g}$ establece un morfismo de monoides

$$\mathcal{g} : (A, \cdot) \rightarrow (A/\sim, \cdot)$$

Resta por ver que + y • definen sobre $A/\sim$ una estructura de anillo, lo cual es consecuencia de ser $\mathcal{g}$ un morfismo sobre de las estructuras de grupo aditivo y monoide multiplicativo. Vamos a demostrar, sin embargo, la validez de la ley distributiva de $\cdot$ respecto de + en $A/\sim$. Sean S, T, U $\in$ $A/\sim$. Sean s, t, u en A tales que $S = \mathcal{g}(s)$, $T = \mathcal{g}(t)$ y $U = \mathcal{g}(u)$. Entonces

$$\begin{aligned}\mathcal{g}(t+u) &= \mathcal{g}(t) + \mathcal{g}(u) = T + U \\ \mathcal{g}(s \cdot t) &= S \cdot T \\ \mathcal{g}(s \cdot u) &= S \cdot U\end{aligned}$$

y por lo tanto

$$\begin{aligned}S \cdot (T + U) &= \mathcal{g}(s \cdot (t + u)) = \mathcal{g}(s \cdot t + s \cdot u) \\ &= \mathcal{g}(s \cdot t) + \mathcal{g}(s \cdot u) \\ &= S \cdot T + S \cdot U\end{aligned}$$

De igual modo probamos la ley distributiva a la derecha. La cuestión sobre unicidad es análoga al caso de grupo cociente. Se dejan a cargo del lector los detalles pertinentes.

2. Por lo visto en la parte 2 del teorema correspondiente para grupos

$$Nu(\mathcal{g}) = \{x / x \sim 0\}$$

y siendo $\sim$ una relación de equivalencia compatible, $N(\mathcal{g})$ es un ideal bilátero. El teorema queda entonces demostrado.

Definición. Con la notación del teorema anterior $A/\sim$ se denomina el <u>anillo cociente</u> de A por la relación de equivalencia $\sim$. Al morfismo $\mathcal{g} : A \rightarrow A/\sim$ se le denomina <u>morfismo canónico</u>. Si I es el ideal bilátero asociado a $\sim$, escribimos también

$$A/\sim \; = A/I$$

Se deja a cargo del lector la demostración de la existencia de isomorfismos

$$A \,/\, \{0\} \simeq A$$
$$A \,/\, A \simeq \{0\}$$

correspondientes a las situaciones $I = \{0\}$ e $I = A$. $\{0\}$ denota el (único) anillo de un solo elemento.

Complementando el teorema anterior se tiene el siguiente.

Teorema. Sea A un anillo y sea I un subgrupo de $(A, +, 0)$. Entonces las siguientes condiciones son equivalentes entre sí:

1) I es ideal bilátero de A.
2) Existe un anillo B y un morfismo $f : A \to B$ tal que

$$Nu(f) = I$$

Demostración

1. ⇒ 2. Es consecuencia del teorema anterior. En efecto, basta tomar $B = A / I$ y ϑ el morfismo canónico.

2. ⇒ 1. $I = Nu(f)$ es un subgrupo de $(A, +, 0)$. Sea $x \in A$ y $c \in I$. Entonces

$$f(x \cdot c) = f(x) \cdot f(c) = f(x) \cdot 0 = 0$$
$$f(c \cdot x) = f(c) \cdot f(x) = 0 \cdot f(x) = 0$$

de manera que

$$x \cdot c \in I \quad y \quad c \cdot x \in I$$

I es pues un ideal bilátero de A.

Ejemplo. Anillos cocientes del anillo de enteros racionales **Z**. Los ideales de **Z** coinciden con los subgrupos de $(\mathbf{Z}, +, 0)$ de manera que las relaciones de equivalencia en **Z** compatibles con la estructura de anillo son las congruencias. Sea $m \in \mathbf{Z}$, $0 < m$. Sea $\mathbf{Z} / (m)$ el grupo cociente de **Z** por el subgrupo (m) de múltiplos de m. Los elementos de $\mathbf{Z} / (m)$ están unívocamente determinados por los restos de la división por m:

$$\mathbf{Z} / (m) = \{\underline{0}, \underline{1}, \ldots, \underline{(m-1)}\}$$

Además, el morfismo canónico

$$\vartheta : \mathbf{Z} \to \mathbf{Z} / (m)$$

está definido por

$$\begin{cases} \vartheta(k) = \underline{r} \\ \text{si } r \text{ es el resto de la división de } k \text{ por } m. \end{cases}$$

De acuerdo con el teorema relativo a anillos cocientes, la estructura de anillo de $\mathbf{Z} / (m)$ está dada por

$$\begin{cases} \underline{r} \cdot \underline{s} = \underline{h} \\ \text{si } h \text{ es el resto de la división de } r \cdot s \text{ por } m. \end{cases}$$

Veamos algunos ejemplos numéricos

$\underline{m = 2.}$ La estructura de anillo de **Z** / (2) está dada por

+	$\underline{0}$	$\underline{1}$
$\underline{0}$	$\underline{0}$	$\underline{1}$
$\underline{1}$	$\underline{1}$	$\underline{0}$

·	$\underline{0}$	$\underline{1}$
$\underline{0}$	$\underline{0}$	$\underline{0}$
$\underline{1}$	$\underline{0}$	$\underline{1}$

$\underline{m = 3.}$ La estructura de anillo de **Z** / (3) está dada por

+	$\underline{0}$	$\underline{1}$	$\underline{2}$
$\underline{0}$	$\underline{0}$	$\underline{1}$	$\underline{2}$
$\underline{1}$	$\underline{1}$	$\underline{2}$	$\underline{0}$
$\underline{2}$	$\underline{2}$	$\underline{0}$	$\underline{1}$

·	$\underline{0}$	$\underline{1}$	$\underline{2}$
$\underline{0}$	$\underline{0}$	$\underline{0}$	$\underline{0}$
$\underline{1}$	$\underline{0}$	$\underline{1}$	$\underline{2}$
$\underline{2}$	$\underline{0}$	$\underline{2}$	$\underline{1}$

En el ejemplo siguiente se unen ambas tablas en una.

$\underline{m = 6.}$ La estructura de anillo de **Z** / (6) está dada por

+ / .	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$	$\underline{4}$	$\underline{5}$
$\underline{0}$	$\underline{0}/\underline{0}$	$\underline{1}/\underline{0}$	$\underline{2}/\underline{0}$	$\underline{3}/\underline{0}$	$\underline{4}/\underline{0}$	$\underline{5}/\underline{0}$
$\underline{1}$	$\underline{1}/\underline{0}$	$\underline{2}/\underline{1}$	$\underline{3}/\underline{2}$	$\underline{4}/\underline{3}$	$\underline{5}/\underline{4}$	$\underline{0}/\underline{5}$
$\underline{2}$	$\underline{2}/\underline{0}$	$\underline{3}/\underline{2}$	$\underline{4}/\underline{4}$	$\underline{5}/\underline{0}$	$\underline{0}/\underline{2}$	$\underline{1}/\underline{4}$
$\underline{3}$	$\underline{3}/\underline{0}$	$\underline{4}/\underline{3}$	$\underline{5}/\underline{0}$	$\underline{0}/\underline{3}$	$\underline{1}/\underline{0}$	$\underline{2}/\underline{3}$
$\underline{4}$	$\underline{4}/\underline{0}$	$\underline{5}/\underline{4}$	$\underline{0}/\underline{2}$	$\underline{1}/\underline{0}$	$\underline{2}/\underline{4}$	$\underline{3}/\underline{2}$
$\underline{5}$	$\underline{5}/\underline{0}$	$\underline{0}/\underline{5}$	$\underline{1}/\underline{4}$	$\underline{2}/\underline{3}$	$\underline{3}/\underline{2}$	$\underline{4}/\underline{1}$

donde los numeradores corresponden a la estructura aditiva y los denominadores a la estructura multiplicativa. Por ejemplo, en la intersección de la fila 3 con la columna 4 se lee $\underline{1}/\underline{0}$. Esto significa

$$\underline{3} + \underline{4} = \underline{1}$$
$$\underline{3} \cdot \underline{4} = \underline{0}$$

Estudiemos algunas propiedades de estos anillos cocientes **Z**/(m), $0 < m$.

i. **Z** / (m) es un anillo conmutativo con identidad.
ii. **Z** / (m) es un cuerpo si, y sólo si, m es primo.

En efecto, sea **Z** / (m) un cuerpo. Entonces si m no es primo podemos escribir $m = r \cdot s$ con $m > r > 1$ y $m > s > 1$. Por lo tanto pasando a **Z** / (m) se tiene

(') $$\underline{r} \cdot \underline{s} = \underline{0}$$

Ahora

$$1 < r < m \Rightarrow \underline{r} \neq \underline{0}$$

(dado que $\underline{r} = \underline{0}$ equivale a ser r divisible por m). Por lo tanto $\underline{r}$ es inversible en $\mathbf{Z} / (m)$. Entonces de (') resulta

$$\underline{0} = \underline{r}^{-1} \cdot (\underline{r} \cdot \underline{s}) = \underline{s}$$

lo cual equivale a que s sea divisible por m. Pero esto es imposible dado que $1 < s < m$. Por lo tanto m es primo.

Recíprocamente, sea m primo. Probemos que $\mathbf{Z} / (m)$ es un cuerpo. Sea en efecto, $\underline{r} \in \mathbf{Z} / (m)$, con $\underline{r} \neq \underline{0}$ o sea $r \in \mathbf{Z}$ satisface

$$0 < r < m$$

m primo implica entonces $(m, r) = 1$. Por propiedades elementales del máximo común divisor existen $t, h \in \mathbf{Z}$ tales que

('') $$1 = (m, r) = t \cdot m + h \cdot r$$

Pasando ('') al anillo cociente resulta

$$\underline{1} = \underline{t'} \cdot \underline{0} + \underline{h'} \cdot \underline{r} = \underline{h'} \cdot \underline{r}$$

(donde con t' y h' hemos indicado los restos de la división de t y h por m). Sigue que $\underline{r}$ es inversible. Ha quedado entonces completamente probado ii.

E. Un Teorema de Isomorfismo

En el capítulo anterior se consideró el problema de la caracterización de los grupos G' que son imágenes de un grupo G por morfismos $f : G \to G'$. El resultado fue que cada tal G' es isomorfo (y en forma natural) al grupo cociente G / H de G por el subgrupo invariante $H = Nu(f)$.

El problema análogo formulado para anillos da lugar al siguiente teorema.

Teorema. Sean A y B anillos y sea $f : A \to B$ un morfismo sobre. Sea

$$I = Nu(f)$$

Existe entonces un único isomorfismo $g : A/I \to B$ con la propiedad de hacer conmutativo el diagrama

(D)
$$\begin{array}{ccc} & A & \\ \mathfrak{g} \swarrow & & \searrow f \\ A/I & \underset{g}{\to} & B \end{array}$$

o sea, tal que

$$g \circ \mathfrak{g} = f$$

Demostración. Según vimos en el teorema análogo para grupos existe un isomorfismo

$$g : (A / I, +, 0) \to (B, +, 0)$$

definido por

$$g(S) = f(s) \quad \text{si} \quad \mathfrak{g}(s) = S$$

Se trata entonces de comprobar que g preserva también la estructura multiplicativa. Sean $S, T \in A / I$ y sean $s, t \in A$ tales que $\mathfrak{g}(s) = S$ y $\mathfrak{g}(t) = T$. Siendo así, sabemos que $\mathfrak{g}(s \cdot t) = S \cdot T$ en A / I. Por lo tanto

$$g(S \cdot T) = f(s \cdot t) = f(s) \cdot f(t) = g(S) \cdot g(T)$$

lo cual prueba nuestra afirmación.

Verifiquemos la unicidad de g. Sea $h : A/I \to B$ un isomorfismo con la propiedad $h \circ \mathfrak{g} = f$. Entonces

$$h \circ \mathfrak{g} = g \circ \mathfrak{g}$$

y siendo $\mathfrak{g}$ un morfismo sobre se tiene la igualdad $h = g$. (En efecto, sea $S \in A/I$ y $s \in S$ con $\mathfrak{g}(s) = S$. Entonces $h(S) = h(\mathfrak{g}(s))$ $= (h \circ \mathfrak{g})(s) = (g \circ \mathfrak{g})(s) = g(\mathfrak{g}(s)) = g(S)$.)

Corolario. Sean A y B anillos y sea $f : A \to B$ un morfismo.

Entonces si $I = Nu(f)$ existe un único <u>monomorfismo</u> $g : A/I \to B$ tal que $g \circ \mathfrak{g} = f$.

Demostración. Ejercicio para el lector.

Ejemplo. <u>Característica en un anillo con identidad.</u> Sea A un anillo con identidad 1. Sea $f : \mathbf{Z} \to A$ la aplicación definida por

$$f(m) = m \cdot 1 \quad \text{si} \quad m \in \mathbf{Z}$$

donde $m \cdot 1$ significa

$$m \cdot 1 = 1 + 1 + \dots + 1 \quad (m \text{ veces}) \text{ si } 0 < m$$
$$m \cdot 1 = 0 \quad \text{si} \quad m = 0$$
$$m \cdot 1 = -((-m) \cdot 1) = -\underbrace{(1 + 1 + \dots + 1)}_{-m \text{ veces}} \text{ si } m < 0.$$

Nótese también, en el caso $m < 0$, la validez de

$$m \cdot 1 = (-1) + (-1) + \dots + (-1) (-m \text{ veces})$$
$$= (-m) \cdot (-1)$$

Vamos a probar que f es un morfismo. Sean $m, n \in \mathbf{Z}$. Consideremos las situaciones siguientes:

i. $0 < m$, $0 < n$. Entonces es claro que $f(m + n) = f(m) + f(n)$.
ii. $m < 0$, $0 < n$. Entonces

$$m \cdot 1 + n \cdot 1 = (-m)\cdot(-1) + n \cdot 1$$
$$\begin{cases} = ((-m)-n)\cdot(-1) \text{ si } n < |m| = \text{valor absoluto de } m \\ = (n-(-m))\cdot 1 \text{ si } |m| < n \end{cases}$$
$$= (m+n)\cdot 1 \text{ en ambos casos.}$$

Por lo tanto $f(m + n) = f(m) + f(n)$

iii. $0 < m$, $n < 0$. Es análoga a ii.
iv. $m < 0$, $n < 0$. Entonces

$$\begin{aligned} m \cdot 1 + n \cdot 1 &= -((-m)\cdot 1) + -((-n)\cdot 1) \\ &= -((-m)\cdot 1 + (-n)\cdot 1) \\ &= -((-m-n)\cdot 1) \\ &= (m+n)\cdot 1 \end{aligned}$$

o sea $f(m + n) = f(m) + f(n)$.

Los casos en que $m = 0$ o $n = 0$ son inmediatos. Se ha probado pues que f es un morfismo de las estructuras aditivas. El lector deberá verificar que $f(m \cdot n) = f(m) \cdot f(n)$. Nótese, además, que $f(1) = 1$.

f es pues un morfismo de las estructuras de anillo. Es importante observar que f es el <u>único</u> morfismo de Z en A. En efecto, otro morfismo $h : Z \to A$ debe satisfacer $h(1) = 1$ y así $h(2) = h(1) + h(1) = 1 + 1 = 2 \cdot 1$, $h(-2) = -h(2) = (-2)\cdot 1$ etc., $h(m) = m \cdot 1$ cualquiera que sea $m \in \mathbf{Z}$, de manera que $h = f$.

Sea entonces $m \in \mathbf{Z}$, $0 \leq m$ tal que $Nu(f) = (m)$. Sigue, en virtud del corolario, la existencia de un monomorfismo $g: \mathbf{Z}/(m) \to A$ tal que el diagrama

$$\begin{array}{ccc} & \mathbf{Z} & \\ q\swarrow & & \searrow f \\ \mathbf{Z}/(m) & \xrightarrow[g]{} & A \end{array}$$

es conmutativo. La unicidad de f, demostrada arriba, y la unicidad de g, dada por el corolario, permiten asociar unívocamente

$$A \to m$$

al anillo A el entero no negativo m. Se denomina m la <u>característica de A</u>. Veamos la propiedad fundamental de m. Sea <u>k un entero tal que $k \cdot 1 = 0$ en A</u>. Entonces

c1) Si $m = 0$ es $k = 0$
c2) Si $m \neq 0$ m divide a k.

En efecto, en la situación c1) $m = 0$ equivale a $0 = (m) = Nu(f)$ por lo tanto

$$k \neq 0 \Rightarrow f(k) \neq 0$$

o sea

$$k \neq 0 \Rightarrow k \cdot 1 \neq 0$$

de manera que

$$k \cdot 1 = 0 \Rightarrow k = 0.$$

En la situación c2),

$$0 = k \cdot 1 = f(k) \Leftrightarrow k \in Nu(f)$$
$$\Leftrightarrow k \in (m)$$
$$\Leftrightarrow m \text{ divide a } k$$

Otras propiedades

- Sea A un anillo (con identidad) de característica $m \neq 0$. Entonces cualquiera que sea $a \in A$ es $m \cdot a = \underbrace{a + a + \ldots + a}_{m \text{ veces}} = 0$. En efecto,

$$\begin{aligned} m \cdot a &= a + a + \ldots + a \\ &= 1 \cdot a + 1 \cdot a + 1 \cdot a \\ &= (m \cdot 1) \cdot a \\ &= 0 \cdot a \\ &= 0 \end{aligned}$$

- Un cuerpo posee característica $m = 0$ o m = primo. Sea A un cuerpo de característica $m \neq 0$. Sea $m = s \cdot t$, $1 \leq s \leq m$, $1 \leq t \leq m$. Ahora en $\mathbf{Z}/(m)$ se tiene

$$\underline{s} \cdot \underline{t} = \underline{m} = \underline{0}$$

por lo tanto

$$g(\underline{s}) \cdot g(\underline{t}) = 0 \text{ en } A$$

y siendo A un cuerpo debe ser

$$g(\underline{s}) = 0 \text{ o } g(\underline{t}) = 0$$

y siendo g un monomorfismo debe ser

$$\underline{s} = \underline{0} \text{ o } \underline{t} = \underline{0}$$

o sea

s múltiplo de m o t múltiplo de m

pero $1 \leq s \leq m$ y $1 \leq t \leq m$. Se sigue que

$$s = m \quad o \quad t = m$$

por lo tanto m es primo.

Ejercicio. Sean A y B anillos con identidad. Sea $C = A \oplus B$ la suma directa de los grupos aditivos correspondientes.

1. Verificar que la ley de composición

$$(a, b) \cdot (a', b') = (a \cdot a', b \cdot b')$$

define sobre $(C, +, 0)$ una estructura de anillo con identidad.

2. Analizar la característica de C en términos de las características de A y B.

3. Determinar la característica de los siguientes anillos:

a) $\mathbf{Z}/(2) \oplus \mathbf{Z}/(2)$
b) $\mathbf{Z}/(2) \oplus \mathbf{Z}/(3)$
c) $\mathbf{Z}/(2) \oplus \mathbf{Z}/(4)$
d) $\mathbf{Z}/(4) \oplus \mathbf{Z}/(6)$
e) $\mathbf{Z} \oplus \mathbf{Z}/(3)$
f) $\mathbf{Z} \oplus \mathbf{Z}$
g) $\mathbf{Z} \oplus \mathbf{Q}$
h) $\mathbf{Z}/(3) \oplus \mathbf{Z}/(5)$

Ejercicio. Sea p un número primo.

1. Probar que en todo anillo conmutativo A, conidentidad de característica p, la aplicación $a \to a^p$ es un endomorfismo. (Sugerencia: utilice la fórmula del binomio y la relación aritmética: $\binom{p}{k} \equiv 0$ (mod p) si $0 < k < p$.)

2. Probar el Teorema de Fermat

$$m^{p-1} \equiv 1 \pmod p \text{ si } (m, p) = 1$$

(Sugerencia: aplique el ejercicio 1 a la situación $A = \mathbf{Z}/(p)$.)

F. Anillos Conmutativos. Anillos de Polinomios

Es interesante destacar una clase de anillos por su importancia en las aplicaciones, especialmente en la geometría algebraica moderna y en la teoría algebraica de números. Nos referimos a los anillos conmutativos o sea aquéllos en los que el producto es conmutativo. Una rama del álgebra los estudia sistemáticamente, a saber, el álgebra conmutativa.

Entre los anillos conmutativos, los más importantes son sin lugar a duda los anillos de polinomios y es nuestra intención hacer aquí un breve estudio. En los cursos elementales de álgebra los polinomios se introducen como: "expresiones formales

$$a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$$

donde los coeficientes $a_0, a_1, \ldots, a_n$ son números y donde X es una cantidad indeterminada". En estos cursos se estudian las operaciones de suma, producto de polinomios y se desarrolla toda una aritmética (divisibilidad, máximo común divisor, algoritmo de división, etc.). En cursos posteriores se hace necesario analizar más detenidamente el papel de la "X". Un método expuesto corrientemente en los libros de álgebra introduce los polinomios con coeficientes en un anillo A como sucesiones

$$(a_0, a_1, \ldots, a_i, \ldots), \quad a_i \in A$$

donde todos los a_i, excepto un número finito, son iguales a 0. La idea subyacente en este método es "sumergir" el anillo A en un anillo (llamémoslo B) que contiene un elemento que hará el papel de la X. Los polinomios no son entonces otra cosa que elementos de B y la

suma y producto de los mismos corresponden a la suma y producto del anillo B.

Vamos a formalizar este punto de vista. Sean A y B anillos conmutativos y sea A subanillo de B. Sea $b \in B$. Llamaremos expresión polinómica en b (con coeficientes en A) a todo elemento, de B, de la forma

$$(P) \qquad a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + \ldots + a_1 \cdot b + a_0$$

donde los $a_0, \ldots, a_n$ son elementos de A que llamaremos coeficientes de la expresión polinómica en b. Por ejemplo, si $A = \mathbf{Z}$ y $B = \mathbf{Q}$ y $b \in \mathbf{Q}$, las siguientes serían expresiones polinómicas en b:

a) $2b - 1$
b) $b^2 - 2$
c) b^3
d) $-b^2 + 3b^3 - 2 + b$
e) 0
f) 5

En efecto, veamos como a), . . , f) se expresan en la forma (P):

a) $2 \cdot b + (-1)$
b) $1 \cdot b^2 + 0 \cdot b + (-2)$
c) $1 \cdot b^3 + 0 \cdot b^2 + 0 \cdot b$
d) $3 \cdot b^3 + (-1)b^2 + b + (-2)$
e) 0 o también $0 \cdot b + 0$ o también $0 \cdot b^2 + 0 \cdot b + 0$, etc.
f) 5 o también $0 \cdot b + 5, \ldots$

Supongamos además que A y B poseen un mismo elemento identidad. Si formamos ahora el conjunto, denotado por A[b], de todas las expresiones polinómicas en b con coeficientes en A es fácil verificar que A[b] es un subanillo de B y además que la suma y producto de expresiones polinómicas en b coinciden con la suma y producto de "polinomios en b" que se han aprendido en cursos elementales. Hay, sin embargo, un detalle relacionado con una propiedad fundamental de polinomios que no hemos mencionado anteriormente:

$$(0) \qquad \begin{cases} a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 = 0 \\ \text{si, y sólo, si } a_n = \ldots = a_0 = 0 \end{cases}$$

Esta propiedad es equivalente al siguiente criterio de igualdad de polinomios. Sean

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0, \quad a_n \neq 0$$
$$g = b_m X^m + b_{m-1} X^{m-1} + \ldots + b_1 X + b_0, \quad b_m \neq 0$$

entonces

$$f = g \text{ si, y sólo si, } n = m \text{ y } a_j = b_j \text{ cualquiera que sea } j, 0 \le j \le m$$

La propiedad (0) es responsable del carácter "formal" de los polinomios, o sea que los polinomios en X sean "lo mismo" que los polinomios en Y.

Volviendo a nuestro esquema de definición tendremos que garantizar la verificación de una propiedad del tipo (0). Por ejemplo, en **Z** ⊂ **Q**, si tomamos $b = 1/2$ se tiene

$$2b - 1 = 0$$

contrario a (0). Por lo tanto, la teoría de polinomios hecha con $b = 1/2$, no sería la adecuada a nuestros fines. Es fácil concluir que ningún número racional serviría para ese fin. Sin embargo, si "sumergimos" **Z** en **R**, se sabe, aunque es difícil de probar, que existen elementos t llamados <u>trascendentes</u>, para los cuales

$$\begin{cases} a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0 = 0 \\ \text{si, y sólo si, } a_n = \ldots = a_0 = 0 \end{cases}$$

(Por ejemplo π y e son trascendentes.) Entonces una teoría de polinomios con coeficientes en **Z** podría desarrollarse sin ambigüedades considerando las expresiones polinómicas en un número trascendente t de **R** con coeficientes en **Z**. Dichas expresiones polinómicas, que en realidad podríamos llamar directamente polinomios en t, no serían otra cosa que números reales y las operaciones entre los mismos más que las operaciones entre números reales. Por lo tanto, una teoría de polinomios con coeficientes enteros es perfectamente admisible.

Para nuestro tratamiento general necesitamos garantizar la existencia de elementos trascendentes, que llamaremos también indeterminadas de acuerdo con la terminología actualmente en uso. Esto lo haremos valiéndonos de la siguiente hipótesis.

Hipótesis. Para todo anillo conmutativo A con identidad existen un anillo conmutativo B con la misma identidad de A y un elemento $X \in B$, tales que

- A es subanillo de B.
- X es trascendente sobre A, en el sentido de (0).

En las condiciones de la hipótesis, consideramos la totalidad de expresiones polinómicas en X con coeficientes en A, conjunto que denotamos por A[X]. Las leyes de composición en B definen sobre A[X] una estructura de anillo. A[X] con esta estructura se denomina el <u>anillo de polinomios en X con coeficientes en A</u>. Explícitamente las leyes de composición en A[X] son:

Sean
$$p(X) = a_n \cdot X^n + a_{n-1} \cdot X^{n-1} + \ldots + a_1 \cdot X + a_0$$
$$q(X) = a'_m \cdot X^m + a'_{m-1} \cdot X^{m-1} + \ldots + a'_1 \cdot X + a'_0$$

(Sin pérdida de generalidad puede suponerse $n = m$, dado que si, por ejemplo, $n < m$, podemos escribir

$$p(X) = 0 \cdot X^m + \ldots + 0 \cdot X^{n+1} + a_n \cdot X^n + \ldots + a_1 \cdot X + a_0).$$

Entonces

$$p(X) + q(X) = s_m \cdot X^m + \ldots + s_i \cdot X^i + \ldots + s_0$$

$$\text{donde } s_i = a_i + a'_i, \; i = o, \ldots, m$$

$$p(X) \cdot q(X) = r_{n+m} \cdot X^{n+m} + \ldots + r_i \cdot X^i + \ldots + r_0$$

$$\text{donde } r_i = a_i \cdot a'_0 + a_{i-1} \cdot a'_1 + \ldots + a_1 \cdot a'_{i-1} + a_0 \cdot a'_i$$

$$i = o, \ldots, m + n$$

En esta forma la introducción del anillo de polinomios $A[X]$ se efectúa sin ambigüedaddes. La dificultad radica en admitir la existencia de anillos B y elementos X como se ha hecho en la hipótesis. Sin embargo, no es difícil de probar la existencia de indeterminadas sobre un anillo conmutativo y en la mayoría de tratados sobre álgebra, donde se hace un tratamiento riguroso de la teoría de polinomios, pueden obtenerse los detalles pertinentes. (Véase, por ejemplo, la referencia bibliográfica (7).)

De ahora en adelante al hablar de polinomios en X con coeficientes en un anillo A nos referiremos al conjunto $A[X]$ con las leyes de composición usuales y omitiremos toda mención del anillo B. Un elemento importante en esta teoría que juega el papel del valor absoluto en el caso del anillo Z es el grado de un polinomio.

Definición. Sea $p(X) = a_n X^n + \ldots + a_1 X + a_0$. Diremos que p(X) tiene grado m

$$gr(p(X)) = m$$

si

$$\begin{cases} a_m \neq 0 \\ m < i \Rightarrow a_i = 0 \end{cases}$$

Si p(X) posee grado m, se llama coeficiente director de p(X) al elemento a_m. Si $a_m = 1$ se dice que p(X) es un polinomio mónico.

Se sigue de la definición que el grado de un polinomio es un entero positivo o nulo y que todo polinomio que tiene grado difiere del polinomio nulo. A este último no se le asigna ningún grado. Las propiedades del grado son las siguientes:

1. $0 \leq gr(p(X))$
2. $gr(p(X)) = 0 \Leftrightarrow p(X) \in A$
3. $gr(p(X) + q(X)) \leq$ máximo $\{gr(p(X)), gr(q(X))\}$ si $p(X) + q(x) \neq 0$
4. $gr(p(X) \cdot q(X)) \leq gr(p(X)) + gr(q(X))$, si $p(X) \cdot q(X) \neq 0$.

donde p(X) y q(X) denotan polinomios no nulos.

Es muy importante la siguiente variante de 4.

Proposición. En 4 vale la igualdad si, y sólo si, $a_n \cdot a'_m \neq 0$, donde $n = gr(p(X))$ y $m = gr(q(X))$. (a_n y a'_m son los coeficientes directores de $p(X)$ y $q(X)$, respectivamente.)

Demostración. La demostración es consecuencia del análisis de los coeficientes del polinomio producto.

Corolario (Importante). Si A es un cuerpo, entonces en A[X]:

$$p(X) \cdot q(X) = 0 \Leftrightarrow p(X) = 0 \quad o \quad q(X) = 0$$

Demostración. $\Leftarrow$ es trivial. Recíprocamente, si fuera $p(X) \neq 0$ y $q(X) \neq 0$, entonces en virtud de la proposición anterior aplicable a nuestra situación por ser A un cuerpo:

$$gr(p(X) \cdot q(X)) = gr(p(X)) + gr(q(X)) \geq 0$$

por lo tanto $p(X) \cdot q(X) \neq 0$.

Mencionemos finalmente la existencia de algoritmo de división en el anillo de polinomios con coeficientes en un cuerpo.

Teorema. Sea K un cuerpo y sea K[X] el anillo de polinomios con coeficientes en el cuerpo K. Sea $p(X) \in K[X]$, $p(X) \neq 0$. Si $q(X) \in K[X]$ existen $t(X)$, $r(X) \in K[X]$ tales que

a) $q(X) = t(X) \cdot p(X) + r(X)$
b) $r(X) = 0$ o $gr(r(X)) < gr(p(X))$

$t(X)$ y $r(X)$ están unívocamente determinados por a) y b).

La demostración es enteramente análoga al caso de existencia de algoritmo de división en **Z**.

Es importante notar que la hipótesis que K sea un cuerpo es esencial; por ejemplo, en el anillo **Z**[X] de polinomios con coeficientes enteros no existe algoritmo de división. En efecto, si $p(X) = 2X$ y $q(X) = X$ no existen $t(X)$, $r(X)$ en **Z**[X] tales que

$$X = t(X) \cdot 2X + r(X)$$

(si a es el coeficiente director de $t(X)$ tendría que satisfacerse $1 = a \cdot 2$, lo cual es imposible,.. en **Z**...).

Ejemplo

Sea $A = \mathbf{Z}/(4)$ y sean $p(X) = \underline{2} \cdot X + \underline{2} = q(X)$. Entonces

$$p(X) + q(X) = 0$$
$$p(X) \cdot q(X) = 0$$

Sean $p(X) = \underline{2} \cdot X^3 + X + \underline{1}$, $q(X) = \underline{2} \cdot X^3 + \underline{1}$. Entonces

$$p(X) + q(X) = X + \underline{2}$$
$$p(X) \cdot q(X) = \underline{2} \cdot X^3 + X + \underline{1}$$

Ejemplo: Anillo de enteros de Gauss. Sean $A = \mathbf{Z}$ y $B = \mathbf{C}$. Sea

$$b = i \in \mathbf{C}$$

($i^2 = -1$). El anillo $Z[i]$ de expresiones polinómicas en i, con coeficientes en Z, se denomina el anillo de enteros de Gauss. Puesto que las potencias de i satisfacen

$$i^2 = -1, \; i^3 = -i, \; i^4 = 1, ..$$

los elementos de $\mathbf{Z}[i]$, poseen la forma

$$m + n \cdot i, \quad m, n \in Z$$

Sea ahora $\mathbf{Z}[X]$ el anillo de polinomios en X con coeficientes en $\mathbf{Z}$. La aplicación (llamada especialización de X por i)

$$p(X) = a_n X^n + .. + a_1 X + a_0 \to p(i) = a_n i^n + .. + a_1 + a_0$$

define un morfismo sobre

$$\mathbf{Z}[X] \to \mathbf{Z}[i]$$

cuyo núcleo es el ideal $I = (X^2 + 1)$ de múltiplos (en $\mathbf{Z}[X]$) del polinomio $X^2 + 1$. En efecto, es claro que

$$(X^2 + 1) \subset I$$

Recíprocamente, sea $p(X) \in I$ y sea

(U) $\quad p(X) = (X^2 + 1) \cdot r(X) + s(X)$
$\quad r(X)$ y $s(X) \in \mathbf{Z}[X]$
$\quad s(X) = 0$ o $gr(s(X)) < 2$

(Dejamos a cargo del lector la justificación del paso anterior.)

Especializando X por i resulta

$$0 = p(i) = 0 + s(i)$$

lo cual dice que i es raíz de $s(X)$. De la teoría elemental de ecuaciones sigue que $-i$ = conjugado de i, es también raíz de $p(X)$. Por lo tanto, $s(X)$ es divisible por

$$(X - i) \cdot (X + i) = X^2 + 1$$

Esto implica, luego de (U) que $p(X) \in (X^2 + 1)$, o sea $I \subset (X^2 + 1)$. En definitiva, $I = (X^2 + 1)$. Por lo tanto, el isomorfismo

$$\boxed{\mathbf{Z}[i] \simeq \mathbf{Z}[X]/(X^2 + 1)}$$

G. Dominios de Integridad. Cuerpo de Cocientes

Definición. Un anillo conmutativo A se denomina un dominio de integridad si $x \cdot y = 0$ en A y si, y sólo si, $x = 0$ o $y = 0$.

Estos anillos son muy importantes en aritmética, heurísticamente podríamos afirmar que son la generalización natural del anillo Z de los enteros racionales.

Ejemplos

1. **Z**.
2. Todo cuerpo es un dominio de integridad.
3. Si A es un dominio de integridad, entonces A[X] es un dominio de integridad. Por lo tanto, **Z**[X], **Q**[Z], **R**[Z], **C**[X] son dominios de integridad.

Otros ejemplos pueden obtenerse a partir del siguiente teorema que dá una condición necesaria y suficiente para que el anillo cociente A/I de un anillo conmutativo sea un dominio de integridad.

Teorema. Sea A un anillo y sea I un ideal de A. Entonces las dos condiciones siguientes sobre I son equivalentes entre sí.

p1) A/I es un dominio de integridad.
p2) $u, v \in A$ y $u \cdot v \in I \Rightarrow u \in I$ o $v \in I$

Demostración. p1) ⇒ p2). Sean $u, v \in A$ con $u \cdot v \in I$. Si $g : A \to A/I$ denota el morfismo canónico, entonces

$$\begin{aligned} u \cdot v \in I &\Leftrightarrow 0 = g(u \cdot v) = g(u) \cdot g(v) \\ &\Leftrightarrow g(u) = 0 \text{ o } g(v) = 0 \quad \text{(por p1)} \\ &\Leftrightarrow u \in I \text{ o } v \in I \end{aligned}$$

p2) ⇒ p1). Sean $S, T \in A/I$ y sean $s, t \in A$ tales que $g(s) = S$ y $g(t) = T$. Entonces

$$\begin{aligned} S \cdot T = 0 &\Leftrightarrow 0 = g(s) \cdot g(t) = g(s \cdot t) \\ &\Leftrightarrow s \cdot t \in I \\ &\Leftrightarrow s \in I \text{ o } t \in I \quad \text{(por p2))} \\ &\Leftrightarrow g(s) = 0 \text{ o } g(t) = 0 \\ &\Leftrightarrow S = 0 \text{ o } T = 0. \end{aligned}$$

El teorema queda demostrado.

Definición. Un ideal I de un anillo conmutativo A que satisface las condiciones del teorema y es además distinto de A se denomina ideal primo.

Ejemplo. En el anillo **Z** de enteros racionales los ideales primos I son exactamente éstos:

(P) $\qquad I = (0)$ e $I = (p)$, p primo

Que los ideales (P) son primos sigue en efecto de

$$\mathbf{Z}/(0) \simeq \mathbf{Z} \quad \text{y} \quad \mathbf{Z}/(p) \text{ es cuerpo}$$

y del teorema anterior. Recíprocamente, sea $I = (m)$ un ideal primo. Si $m = 0$ no hay nada que probar. Si $m \neq 0$ y es $m = r \cdot s$, $0 < r$, $0 < s$, entonces $m \in I$ implica $r \in I$ o $s \in I$. Sea $r \in I$, entonces $I = (m)$ implica $r = k \cdot m$, $k \in Z$. Por lo tanto

$$m = r \cdot s = k \cdot m \cdot s$$

y siendo $0 \neq m$ es $1 = k \cdot s$ y la única posibilidad de s es $s = 1$. Por lo tanto, la única factorización de m es $1 \cdot m$, m es entonces primo.

Ejemplo. Sea $\mathbf{R}$ el cuerpo de los números reales y sea $A = \mathbf{R}[X]$ el anillo de polinomios en X con coeficientes reales. Sea $I \subset A$ definido por

$$I = (X^2 + 1) = (X^2 + 1) \cdot \mathbf{R}[X]$$

o sea I es la totalidad de múltiplos, en A, del polinomio $X^2 + 1$.

Afirmación. I es ideal primo de A. Es de inmediata verificación que I es ideal de A. Sean $t(X)$, $v(X) \in A$ tales que $t(X) \cdot v(X) \in I$. Existe entonces $r(X) \in A$ tal que

(I) $$t(X) \cdot v(X) = (X^2 + 1) \cdot r(X)$$

Ahora, en virtud del algoritmo de división en $\mathbf{R}[X]$, podemos escribir

(II) $$\begin{aligned} t(X) &= (X^2 + 1) \cdot h(X) + s(X) \\ v(X) &= (X^2 + 1) \cdot g(X) + w(X) \end{aligned}$$

donde $s(X)$ y $w(X)$ satisfacen

$$\begin{aligned} s(X) &= 0 \quad \text{o} \quad gr(s(X)) < 2 \\ w(X) &= 0 \quad \text{o} \quad gr(w(X)) < 2 \end{aligned}$$

Si fuera $s(X) = 0$ entonces $t(X)$ sería múltiplo de $X^2 + 1$, o sea $t(X) \in I$ y no habría nada que probar. Análogamente, si $w(X) = 0$. Por lo tanto, supongamos que $s(X)$ y $w(X)$ poseen grado menor que 2. Se sigue que

(III) $$gr(s(X) \cdot w(X)) \leq 2$$

Efectuando el producto $t(X) \cdot v(X)$ según (II) y comparando con (I) resulta

$$s(X) \cdot w(X) \in I \text{ o sea } s(X) \cdot w(X) = (X^2 + 1) \cdot j(X)$$

Sin embargo, por razones de grado (véase (III)) debe ser

$$gr(j(X)) = 0 \text{ o sea } j(X) = q \in R$$

Sin pérdida de generalidad podemos suponer $j(X) = q = 1$. En definitiva se tiene

(IV) $$s(X) \cdot w(X) = X^2 + 1$$

y siendo ahora $gr(s(X)) \leq 1$ y $gr(w(X)) \leq 1$ se tiene

$$gr(s(X)) = 1 \quad \text{o sea} \quad s(X) = aX + b, \; a \neq 0$$
$$gr(w(X)) = 1 \quad \text{o sea} \quad w(X) = cX + d, \; c \neq 0$$

Escribiendo (IV)

$$(aX + b) . (cX + d) = X^2 + 1$$

resulta

$$ac = bd = 1 \quad y \quad ad + bc = 0$$

por lo tanto

$$a^2 + b^2 = a^2(bd) + b^2(ac) = ab(ad + bc) = 0$$

una contradicción, ya que $a \neq 0$. Ha quedado confirmada nuestra afirmación que I es ideal primo de A.

De acuerdo con el teorema que se acaba de probar se tiene que A/I es un dominio de integridad. Vamos a caracterizarlo. Sea $p(X) \in A$. Entonces, en virtud del algoritmo de división de polinomios existen únicos polinomios $s(X)$ y $r(X)$ tales que

$$p(X) = (X^2 + 1) \cdot s(X) + r(X)$$

donde $\quad r(X) = 0 \text{ o } gr(r(X)) \leq 1$

La condición $r(X) = 0$ o $gr(r(X)) \leq 1$ puede expresarse también diciendo que $r(X)$ es un polinomio de la forma

$$r(X) = bX + a$$

donde a, b son números reales determinados por $p(X)$.

Nótese además que si

$$q(X) = (X^2 + 1) \cdot s'(X) + (bX + a)$$

entonces $p(X) - q(X) \in I$, de manera que si $\mathcal{g} : A \to A/I$ denota el morfismo canónico se tiene

$$\mathcal{g}(p(X)) = \mathcal{g}(q(X)) = \mathcal{g}(bX + a)$$

o sea

$\mathcal{g}(p(X))$ está unívocamente determinado por el par ordenado (a, b) de coeficientes del polinomio $bX + a$, resto de la división de $p(X)$ por $X^2 + 1$.

De acuerdo con lo precedente, los elementos de A/I los denotaremos por pares (a, b).

Es interesante considerar ahora cómo se opera en A / I de acuerdo con estos pares. Sean pues $(a, b), (c, d) \in A/I$. Entonces

$$\mathcal{g}(a + bX) = (a, b) \quad y \quad \mathcal{g}(c + dX) = (c, d)$$

Por lo tanto

$$(a, b) + (c, d) = \mathcal{g}(a + bX) + \mathcal{g}(c + dX) = \mathcal{g}((a + c) + (b + d)X)$$
$$= (a + c, b + d)$$

$$
\begin{aligned}
(a, b) \cdot (c, d) &= \varphi(a + bX) \cdot \varphi(c + dX) \\
&= \varphi(a + bX) \cdot (c + dX) \\
&= \varphi((ac - bd) + (ad + bc)X + bd(X^2 + 1)) \\
&= \varphi((ac - bd) + (ad + bc)X) \\
&= (ac - bd,\ ad + bc)
\end{aligned}
$$

La estructura obtenida así en A/I no es otra cosa que el anillo (o mejor dicho, el cuerpo) **C** de los números complejos.

Las propiedades fundamentales de los dominios de integridad están ligadas a propiedades bien conocidas del anillo **Z** de enteros racionales. Una primera propiedad es la posibilidad de "sumergir" un dominio de integridad A en un cuerpo cuyos elementos son "cocientes" de elementos de A. Esto corresponde a la construcción del cuerpo **Q** de fracciones de elementos en **Z**. Una segunda propiedad es la teoría general de la divisibilidad, existencia de algoritmos de división, etc. La primera propiedad se resume en un teorema que vamos a enunciar a continuación. La segunda es mucho más compleja y da lugar al estudio de estructuras particulares, como son los dominios de factorización única, los dominios euclidianos, los dominios de ideales principales. *

Teorema de Inmersión de un Dominio de Integridad en un Cuerpo de Cocientes. Sea A un dominio de integridad.

1) Existe un cuerpo D y un monomorfismo

$$\varphi : A \rightarrow D$$

tal que para todo $d \in D$ existen $r, s \in A$ que satisfacen

$$s \neq 0 \quad y \quad d = \varphi(r) \cdot \varphi(s)^{-1}$$

2) Si D^* es un cuerpo y $\varphi^* : A \rightarrow D^*$ con las mismas propiedades que en 1). Existe un isomorfismo

$$\psi : D \rightarrow D^*$$

tal que el diagrama

$$
\begin{array}{ccc}
 & A & \\
\varphi \swarrow & & \searrow \varphi^* \\
D & \underset{\psi}{\rightarrow} & D'
\end{array}
$$

es conmutativo.

Demostración

1. La demostración se hace repitiendo el esquema de construcción de los números racionales a partir de los números enteros. Los detalles se dejan a cargo del lector.

---

* Véase, por ejemplo, Zariski-Samuel, Commutative Algebra, Vol. 1, pags. 21-24, 242-247 (1958).

2. Sean D, D*, $\dot{g}$, $\dot{g}^*$ como en 1) y 2). Sea $x \in D$. Existen entonces $r, s \in A$, $s \neq 0$ tales que $\dot{g}(r) \cdot \dot{g}(s)^{-1} = x$. Si además tuviéramos $x = \dot{g}(r') \cdot \dot{g}(s')^{-1}$, $r', s' \in A$, $s' \neq 0$ se tendría

$$\dot{g}(r) \cdot \dot{g}(s)^{-1} = \dot{g}(r') \cdot \dot{g}(s')^{-1}$$

o sea

$$\dot{g}(r) \cdot \dot{g}(s') = \dot{g}(r') \cdot \dot{g}(s)$$
$$\dot{g}(r \cdot s') = \dot{g}(r' \cdot s)$$

y siendo $\dot{g}$ un monomorfismo, se tendrá

$$r \cdot s' = r' \cdot s$$

Por lo tanto

$$\dot{g}^*(r) \cdot \dot{g}^*(s') = \dot{g}^*(r \cdot s') = \dot{g}^*(r' \cdot s) = \dot{g}^*(r') \cdot \dot{g}^*(s)$$

de manera que

$$\dot{g}^*(r) \cdot \dot{g}^*(s)^{-1} = \dot{g}^*(r') \cdot \dot{g}^*(s')^{-1}$$

lo cual demuestra que

$$x \to \dot{g}^*(r) \cdot \dot{g}^*(s)^{-1}$$
$$\text{si } x = \dot{g}(r) \cdot \dot{g}(s)^{-1}$$

define una aplicación

$$\dot{\psi} : D \to D^*$$

que satisface, si $a \in A$ y $b \neq 0$ en A,

$$\begin{aligned}(\dot{\psi} \circ \dot{g})(a) &= \dot{\psi}(\dot{g}(a)) = \dot{\psi}(\dot{g}(a \cdot b) \cdot \dot{g}(b)^{-1}) \\ &= \dot{g}^*(a \cdot b) \cdot \dot{g}^*(b)^{-1} = \dot{g}^*(a) \cdot \dot{g}^*(b) \cdot \dot{g}^*(b)^{-1} \\ &= \dot{g}^*(a)\end{aligned}$$

de manera que

$$\dot{\psi} \circ \dot{g} = \dot{g}^*$$

que demuestra la conmutatividad del diagrama anterior.

Falta por demostrar que $\dot{\psi}$ es un morfismo de anillos y, además, que es un isomorfismo. Se encomienda al lector su verificación.

Definición. Un cuerpo D con las propiedades dadas en el teorema se denomina un cuerpo de cocientes de A. Si D es un cuerpo de cocientes de A se suele identificar A con un subanillo de D por medio del monomorfismo $\dot{g}$. Los elementos de D se escriben entonces $r \cdot s^{-1}$, $r, s \in A$, $s \neq 0$ o también por medio de fracciones r/s.

La segunda parte del teorema demuestra que todos los cuerpos de cocientes de un dominio de integridad son isomorfos entre sí, siendo el isomorfismo "natural" en el sentido que existe un diagrama conmutativo, como el señalado en el teorema. Este isomorfismo de los diferentes cuerpos de cocientes se expresa técnicamente diciendo que todo dominio de integridad posee esencialmente un cuerpo de cocientes o también que un dominio de integridad posee un único cuerpo de cocientes, salvo un isomorfismo. Se habla

entonces del cuerpo de cocientes del dominio en cuestión. Note el lector que si en particular A es un cuerpo, entonces A es su propio cuerpo de cocientes.

Ejercicios

1. Sea K un cuerpo y sea A un subanillo de K, con identidad.

   i. Probar que la identidad de A coincide con la identidad de K.
   ii. Probar que A es un dominio de integridad.
   iii. Probar que K es cuerpo de cocientes de A si, y sólo sí, se satisface la condición siguiente: Para todo $k \in K$ existe $a \in A$, $0 \neq a$ tal que $k \cdot a \in A$.

2. ¿Es **R** cuerpo de cocientes de **Z**?

3. Sea $A = \mathbf{Z}[i]$ el anillo de enteros de Gauss. Probar que el subanillo $D = \mathbf{Q}[i]$ de **C** de expresiones polinómicas en i ($i^2 = -1$) con coeficientes racionales es cuerpo de cocientes de A.

4. Sea $A = \mathbf{Z}[\sqrt{2}]$ el subanillo de **R** de expresiones polinómicas en $\sqrt{2}$ con coeficientes enteros. Probar que el subanillo $D = \mathbf{Q}[\sqrt{2}]$ de **R** de expresiones polinómicas en $\sqrt{2}$ con coeficientes racionales es cuerpo de cocientes de A.

5. Sea K un cuerpo y sea K[X] el anillo de polinomios con coeficientes en K. Describir un cuerpo de cocientes de K[X].

BIBLIOGRAFIA

(1) BIRKHOFF, G. y MACLANE, S. A Survey of Modern Algebra, Macmillan, Nueva York (1953).

(2) BOURBAKI, N. Algèbre, Éléments de Mathématique, Tomo II, Cáp. I, Actualités Scientifiques et Industrielles, París (1958).

(3) CLIFFORD, A.H. y PRESTON, G. B. The Algebraic Theory of Semigroups, Vol. I, Mathematical Surveys N° 7, American Mathematical Society (1961).

(4) DUBREIL, P. Algèbre, Gauthier-Villars, París (1954).

(5) GENTILE, E.R. Notas de Algebra, Cursos y Seminarios de Matemática, Fasc. 22, Universidad de Buenos Aires, Facultad de Ciencias Exactas, Buenos Aires (1965).

(6) JACOBSON, N. Lectures in Abstract Algebra, Vol. I, Van Nostrand, Princeton, N.J. (1953).

(7) MOSTOW, D.D., SAMPSON, J.H. y MEYER, J.P. Fundamental Structures of Algebra, McGraw, Nueva York (1963).

(8) OUBIÑA, L. Introducción a la Teoría de Conjuntos, EUDEBA, Buenos Aires (1965).

(9) ROTMAN, J.J. The Theory of Groups, An Introduction, Allyn and Bacon, Boston, Mass. (1965).

(10) ZARISKI, O. y SAMUEL, P. Commutative Algebra, Vol. I, Van Nostrand, Princeton, N.J. (1958).

Nota. - Con respecto a las referencias bibliográficas relativas a cada capítulo de esta monografía, véase para:

Introducción - referencia 8.
Capítulo I - referencias 2, 4, 6 y 3 (profundizan el tema de semigrupo y sus aplicaciones).
Capítulo II - referencias 1, 2, 5, 6, 7, 8 y 9.
Capítulo III - referencias 1, 2, 5, 6, 7 y 10.

COLECCION DE MONOGRAFIAS CIENTIFICAS

Publicadas

Serie de matemática

N° 1. La Revolución en las Matemáticas Escolares, por el Consejo Nacional de Maestros de los Estados Unidos de América.
N° 2. Espacios Vectoriales y Geometría Analítica, por Luis A. Santaló.
N° 3. Estructuras Algebraicas, por Enzo R. Gentile.

Serie de física

N° 1. Concepto Moderno del Núcleo, por D. Allan Bromley.
N° 2. Panorama de la Astronomía Moderna, por Félix Cernuschi y Sayd Codina.

Serie de química

N° 1. Cinética Química Elemental, por Harold Behrens Le Bas.

Serie de biología

N° 1. La Genética y la Revolución en las Ciencias Biológicas, por José Luis Reissig.
N° 2. Bases Ecológicas de la Explotación Agropecuaria en la América Latina, por Guillermo Mann F.

En preparación

Serie de matemática

Algebra Lineal, por Orlando Villamayor.
Algebra Linear e Geometria Euclidiana, por Alexandre Martins Rodrigues.
Funções Reais de Variável Real, por Djairo Guedes de Figueiredo.
Números Reales y Complejos, por César A. Trejo.
Historia de las Ideas Modernas en la Matemática, por José Babini.
Programación Lineal, por Enrique Cansado.
Introducción a la Topología, por Juan Horváth.
Aplicaciones de la Topología, por José Nieto.

Serie de física

Física de Partículas, por Igor Saavedra.
La Estructura Electrónica de los Sólidos, por Leopoldo M. Falicov.
Física Nuclear, por Mariano Bauer E. y Alfonso Mondragón.
Física Cuántica, por Thomas A. Brody.
Experimento y Teoría en la Enseñanza de la Física al Nivel Secundario, por Félix Cernuschi.
Nuevas Orientaciones en la Enseñanza de la Física, por Darío Moreno.

Serie de química

Mecanismos de Reacciones, por Jorge Brieux.
Elementos Encadenados, por Jacobo Gómez Lara.
Macromoléculas, por Alejandro Paladini y M. Burachik.
Bioenergética, por Isaias Raw y Walter Colli.
Enseñanza de la Química Experimental, por Francisco Giral.
Complejos, por Manuel Madrazo Garamendi.

Serie de biología

Cómo Enseñar Biología, por Oswaldo Frota-Pessoa.
La Célula, por Renato Basile.
Microorganismos, por J. M. Gutiérrez-Vázquez.
La Taxonomía y la Revolución en las Ciencias Biológicas, por Elías R. de la Sota.